Microsoft

Building Global Trust Online, 4th Edition

Microsoft Perspectives for Policymakers

Security

Privacy

Online Safety

Accessibility

Thank you for taking the time to explore *Building Global Trust Online, 4th Edition: Microsoft Perspectives for Policymakers*. We hope you find it to be a valuable resource to address the many online issues that confront policymakers today.

As technology becomes increasingly important in day-to-day living—for work, commerce, and communication—it is vital that everyone, regardless of ability or age, be able to enjoy the benefits of the digital world. However, the technological tools created for the betterment of society are also being used as instruments for crime and malicious intent. Security, privacy, and online safety often top the list of concerns for businesses, governments, and individuals the world over. The Microsoft approach to these issues is called Trustworthy Computing, a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone.

Building Global Trust Online is intended to be a relevant and useful guide for any decision-maker who is responsible for developing new ideas and solutions for security, privacy, online safety, and accessibility. This publication relies on extensive work and ongoing research by internal teams at Microsoft as well as consultation with external subject-matter experts. We appreciate the scope and changing complexities of these issues—as well as the tremendous value of collaborative efforts to provide the most up-to-date information, support, and guidance.

Within *Building Global Trust Online, 4th Edition*, you will find overviews of key issues; a summary of the Microsoft response to these issues, including products, services, and global collaborative efforts; recommended policy considerations; infographics and data visualizations; and a list of helpful resources for further reading and review. We've provided information about topics such as:

- Current efforts and resources used to address, mitigate, or eliminate today's cyberthreats
- Future privacy models to improve current practices and address privacy concerns
- Issues related to the protection of youth online
- The Microsoft commitment to innovative accessibility solutions
- Microsoft products, services, partnerships, and ongoing work to promote a safer, more trusted Internet

The full 120-page publication and the individual booklets of Security, Privacy, Online Safety, and Accessibility are available on our Policymaker website at **www.microsoft.com/policymakers**.

We hope you will find *Building Global Trust Online, 4th Edition: Microsoft Perspectives for Policymakers* a useful resource in helping bring about a more trusted computing experience and a safer, more secure Internet for everyone.

Microsoft Trustworthy Computing

Contents

Microsoft Trustworthy Computing 4

SECURITY 7

Making Computing More Secure for Everyone 9
Cybersecurity 10
Cybersecurity Norms 12
National Strategies for Cybersecurity 14
Collective Defense: Applying Public Health Models to Internet Security 16
Combating Botnets 18
Critical Infrastructure Protections 20
Data Breach Notification 22
Supply Chain Security 24
Microsoft Malware Protection Center 26
Microsoft Security Intelligence Report 28
Microsoft Security Development Lifecycle 30
Microsoft Security Response Center 32
Resources 34

PRIVACY 37

Our Commitment to Privacy 39
Privacy 40
Baseline Privacy Legislation 42
Future Privacy Models 44
Microsoft Privacy Statements 46
Privacy Accountability 48
Privacy by Design at Microsoft 50
Privacy in the Cloud 52
Resources 55

ONLINE SAFETY 57

Online Safety at Microsoft: Building a Safer Digital World 59
Online Safety 60

Digital Citizenship 62
Child Online Safety 64
Online Safety Education 67
Family Safety Settings 69
Microsoft Computing Safety Index 71
Combating Child Exploitation Online 74
Combating Child Grooming Online 76
Combating Human Trafficking Online 78
Combating Online Bullying 81
Combating Online Fraud 83
Safer Online Gaming 85
Online Reputation 88
Online Safety for Mobile Devices 90
Safer Social Networking 92
Internet Security at Work 94
Global Online Safety Partnerships and Initiatives 97
Resources 99

ACCESSIBILITY 103

Who Benefits from Accessible Technology — and How Great Is the Need? 105
Accessibility 106
Accessibility and People-Centric Design 108
Accessibility and the Cloud 110
Accessibility in Education 112
An Association of Accessibility Professionals 114
Implementing the U.N. Convention on the Rights of Persons with Disabilities 116
Technology and Older Adults 118
Resources 120

Key Points

- In 2002, Bill Gates outlined three key tenets that still define trustworthy computing today: security, privacy, and reliability. But the role of computers in everyday life is changing, and each of these aspects must be fundamentally redefined to meet new challenges.

- Security models need to take a more holistic approach that encompasses prevention, detection, containment, and recovery. Privacy governance needs to replace the current notice and consent model with a framework based on use. Reliability models need to supplement the traditional reliance on data replication and redundancy with a new engineering intelligence that focuses on software that detects, isolates, and repairs outages.

- Governments have a special role in advancing trustworthy computing because they have both the power to catalyze markets through incentives and the ability to dictate behavior through regulation.

On January 15, 2002, Bill Gates launched Trustworthy Computing, a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone.

Since 2002, important changes have occurred in the areas of security, privacy, and reliability. New threats and cyberwarfare have challenged computer security professionals. People are now connected through a host of Internet-enabled applications, creating massive new global data flows that strain the traditional notice and consent model that protects privacy. Reliability must be improved to accommodate the greater dependence on cloud computing, with large-scale systems promising anywhere, anytime access.

The core attributes of trustworthy computing are as important as ever, but this new set of challenges requires innovative solutions.

- To meet the security challenges of increasingly determined and persistent adversaries, organizations should adopt a holistic security strategy that encompasses prevention, detection, containment, and recovery.

- To adjust to the privacy implications of a data-rich world, organizations need to craft principles that protect privacy while reaping the benefits that only the massive aggregation of computer data, or *big data*, can bring.

- Finally, to build the reliability that information and communications technology (ICT) depends on, organizations need to recognize the complexity of evolving ICT systems, and create products and services that can be flexible in times of failure.

Microsoft Approach

Trustworthy Computing addresses the changes to the online world in each of the three aspects of security, privacy, and reliability.

SECURITY: Threats can challenge almost any part of an ICT system, making absolute security impossible. This more dangerous threat environment requires a new model of computer security that consists of prevention, detection, containment, and recovery. While these elements are not new, many organizations have not dedicated their efforts to the strategies necessary to ensure that if part of the network is compromised, the adversary is well contained. Security strategies have also not focused on capturing, correlating, and analyzing audit events from across an enterprise to detect anomalies that reveal attacker movement.

PRIVACY: It is clear that the privacy challenges in a cloud-enabled world cannot be addressed by traditional privacy principles that focus on the collection of data and the notices provided at the time it is collected—a notice and consent privacy model. The use of data serves as a better starting point for defining the obligations

related to personal information. A model based on use is better suited for both the organizations that collect data from individuals and others who may use it. This model requires organizations to be transparent, offer and honor appropriate choices, and ensure that they assess and manage the risks to consumers related to the use of their data.

RELIABILITY: With technology embedded in so many aspects of everyday life, reliability must achieve a level not possible today. To bring this about, two fundamental changes must occur. First, companies must leverage the cloud and its big data to create engineering intelligence—the ability to understand both internal and cross-organizational dependencies. For example, simply watching data flows between networks may reveal significant dependencies that were previously not understood.

Second, organizations need to stop thinking of reliability solely in terms of redundancy and data replication, which are insufficient to ensure high levels of reliability in the cloud. The traditional emphasis placed on preventing failures in software needs to be supplemented by an increased focus on software that detects, isolates, and repairs (or works around) failures associated with composite computing systems.

Microsoft recognizes that there are many issues beyond security, privacy, and reliability that affect people's trust in computing. One such issue is accessibility. As technology becomes increasingly important in day-to-day living—for work, commerce, and communication—it is vital that everyone, regardless of ability or age, be able to enjoy the benefits of the digital world. Microsoft is therefore committed to developing innovative accessibility solutions through four key areas of focus: product accessibility, leadership and awareness, innovation, and collaboration.

Policy Considerations

- **RECOGNIZE GOVERNMENT'S SPECIAL ROLE IN PROTECTING THE INTERNET** Governments have both the power to catalyze markets through incentives and the ability to dictate behavior through regulation. Governments also play a unique role in responding to online threats from enforcing criminal laws to protecting a nation from military attacks.

- **ESTABLISH NORMS FOR COLLABORATION BETWEEN PUBLIC AND PRIVATE SECTORS** As governments construct cybersecurity practices to address security concerns at the international level, they should seek input from a variety of stakeholders, including the private sector, civil society, and academia.

- **ESTABLISH RULES FOR INTERNATIONAL DATA ACCESS BY GOVERNMENTS** Governments need to agree upon a new framework for international assistance that goes beyond traditional mutual legal assistance treaties. Under a new framework, countries could agree that there should be a formal process for accessing data.

- **SUPPORT COMPREHENSIVE PRIVACY LEGISLATION** Legislation should apply both online and offline and include requirements for transparency, consumer control, and security. Legislation should preempt state or local laws that are inconsistent with federal requirements. It should also ensure that businesses use, store, and share data responsibly, while encouraging competition on the basis of more robust privacy practices.

Microsoft

Security

Building Global Trust Online, 4th Edition

Microsoft Perspectives for Policymakers

Making Computing More Secure for Everyone

Cybersecurity spans from a single mobile phone up to critical government operations across scores of devices — modern security regulations are needed to cover all scales of network use.

The need for public policy

In a 2011 experiment, the US Department of Homeland Security dropped "malware-infected" USBs in agency and contractor parking lots[1]

This reflects a larger trend of vulnerability ranging from conventional crime to cyberwarfare[4]

If truly infected, each drive could have infiltrated critical databases[3]

Microsoft believes nations should implement cybersecurity strategies protecting national security, the economy, and public safety

HOW CAN WE DO THIS WITH PRIVACY, CIVIL LIBERTIES, AND MANAGEABLE COST INTACT?

Principles of effective cybersecurity strategy

RISK-BASED

Assess risk by identifying threats, vulnerabilities, and consequences; manage through mitigations, controls, costs, etc.

PRACTICABLE

Adoption and implementation should be as wide as possible.

OUTCOME-FOCUSED

Instead of prescribing the path to full security, focus on the end goal.

RESPECTFUL OF PRIVACY AND CIVIL LIBERTIES

Include protections based upon critical policies, practices, and frameworks surrounding these issues.

PRIORITIZED

Not all disruptions or failures will be equal across all critical assets or sectors — weigh the priorities.

GLOBALLY RELEVANT

Integrate international standards to the greatest extent possible while harmonizing globally.

We receive monthly cyberthreat data from

+600

MILLION SYSTEMS

= 10 million

in

+100

COUNTRIES AND REGIONS[5]

Read on to learn more about how this knowledge could inform public policies to protect global nations

1 www.gcn.com/articles/2011/06/30/dhs-test-found-thumb-drives-disks-network.aspx | 2 ibid. | 3 Microsoft. Developing a National Strategy for Cybersecurity. | 4 Microsoft. Rethinking Cyber Threats. | 5 Microsoft. Developing a National Strategy for Cybersecurity.

Cybersecurity

Key Points

- Cybersecurity is the set of activities and resources that enable citizens, enterprises, and governments to meet their computing objectives in a secure, private, and reliable manner.
- Governments face the challenge of developing security practices that address four types of threats: conventional cybercrimes, military espionage, economic espionage, and cyberwarfare.
- Microsoft works to help create safer, more trusted computing experiences by continually improving the security of its products and services, developing best practices for cybersecurity, and collaborating with governments and industry partners to reduce threats to cybersecurity.
- An effective approach to cybersecurity requires collaboration between the public and private sectors to mitigate threats and vulnerabilities. This collaboration also helps develop sustainable public policy frameworks that advance cybersecurity and enable innovation in the private sector.

Cybersecurity includes the security of information, operations, and computer systems.

It is the set of activities and resources that enable citizens, enterprises, and governments to meet their computing objectives in a secure, private, and reliable manner.

Cybersecurity means different things to different audiences. For businesses, it is about ensuring, through operational and information security, the availability of critical business functions and the protection of confidential data.

For governments, it is about protecting citizens, enterprise, critical infrastructure, and government computer systems from attack or compromise. Governments face the challenge of developing cybersecurity best practices, which address four categories of threats that have the potential to affect public safety and national security. First, governments must protect society from a broad range of conventional cybercrimes (such as fraud or vandalism) perpetrated by individuals, organized crime syndicates, and loosely affiliated groups of "hacktivists." Countries may also need to combat military espionage that uses computing technologies, as illustrated by repeated allegations of cross-border exfiltration of sensitive military data. Nations must also defend against economic espionage and other such actions where governments have philosophical differences about what constitutes acceptable behavior. Finally, they must grapple with cyberwarfare, forcing a reassessment of traditional notions of war.

With societies around the globe growing ever more dependent on information and communications technologies, the importance of cybersecurity will grow significantly over time. Accordingly, policymakers should think strategically about how to mitigate cyberthreats.

Microsoft Approach

Microsoft manages risk through ongoing efforts to enhance security in product development, the supply chain, and operations, as well as by deepening its understanding of social engineering tactics.

PRODUCT DEVELOPMENT SECURITY To address potential product vulnerabilities, Microsoft uses its Security Development Lifecycle, a security assurance process that relies on a set of mandatory security activities grouped by the phases of traditional software development.

SUPPLY CHAIN SECURITY To help manage risks to its products and services in the supply chain, Microsoft deploys identity and access management controls, the Security Development Lifecycle, policies and procedures that monitor the integrity of Microsoft software, and anti-counterfeit measures.

Microsoft is also actively involved in industry efforts, such as the Software Assurance Forum for Excellence in Code (SAFECode), to develop best practices for managing risk in the supply chain and product assurance tools.

OPERATIONAL SECURITY To help organizations better manage operational security risks, Microsoft shares its security best practices and provides regular software updates. The Microsoft update management system enhances operational security through standard releases of software updates on the second Tuesday of each month.

SOCIAL ENGINEERING DEFENSE Microsoft helps combat social engineering by sharing security best practices and developing instructional materials for consumers. It also provides tools like the Windows Internet Explorer SmartScreen Filter, which helps protect people from evolving social engineering threats.

Building on various internal risk-management programs, Microsoft continually seeks to improve the efficiency and effectiveness of these approaches. Microsoft shares those practices with industry and policymakers as appropriate.

In addition, the Microsoft Global Security Strategy and Diplomacy team partners with national governments, industry partners, and nonprofit organizations to enhance the security of the Internet. To that end, the team promotes trustworthy plans and policies, and helps protect processes key to national and economic security as well as public health, safety, and confidence.

Policy Considerations

Public policymakers can help strengthen cybersecurity and enable security innovation in the private sector by advancing these practices:

- **ENCOURAGE OUTCOME-FOCUSED INITIATIVES AND PARTNERSHIPS** Governments should work with the private sector to strengthen the security, privacy, and reliability of the cyberecosystem and to defend against cyberthreats. Such strategic partnerships and outcome-focused initiatives are critical to advancing a safer Internet.

- **SUPPORT EXISTING FRAMEWORKS AND BEST PRACTICES** In partnership with the private sector, policymakers should build on industry best practices for risk-based, technology-neutral approaches to mitigating cyberthreats. Relying on tested frameworks helps ensure that hard-won security gains are maintained and technological innovations are given maximum opportunity to succeed.

- **CONSIDER LOCAL CONCERNS AND INFRASTRUCTURES** As governments work to advance their national security goals through effective cybersecurity, they should also consider their unique information technology infrastructures. Public-private partnerships can help identify gaps between national security expectations and what commercially available technologies can offer to address areas of specific concern.

Cybersecurity Norms

Key Points

- Conflict in cyberspace, unlike physical warfare, does not have a widely agreed-upon set of conventions (or more significantly, norms) for regulating conflict.
- Microsoft supports a four-step process for driving the development and understanding of global cybersecurity norms and practices forward.
- As governments continue to develop their views on cybersecurity and normative behavior in cyberspace, creating international public-private partnerships can help ensure the resiliency of critical infrastructures and agility in responding to complex security events in cyberspace.

Societies are increasingly dependent on a global network of information and communications technology (ICT) to control the critical infrastructures and communications systems essential to modern life. This dependency will only increase as developing nations build modern ICT infrastructures.

Along with the benefits have come new threats, including:

CYBERCRIME SUCH AS IDENTITY THEFT AND FRAUD

POLITICALLY MOTIVATED ATTACKERS WHO THREATEN CRITICAL INFRASTRUCTURE

SOPHISTICATED ECONOMIC AND MILITARY ESPIONAGE

Technology can also be exploited to cause significant harm at a national level, including, but not limited to, damage to critical infrastructures (energy, communications, banking, transportation, and other systems), theft of intellectual property, exploitation of government systems, and criminal attacks against citizens.

To respond to threats, governments are under a lot of pressure to develop and maintain capabilities for defending the nation in cyberspace, maintaining appropriate intelligence capabilities, enforcing criminal law, and reducing risk in critical infrastructures and the broader economy. Governments are acting to broaden the range of their national security capabilities in cyberspace. A study by the United Nations Institute for Disarmament Research (UNIDIR) in 2011 identified 33 nation states that address cyberwarfare in their military planning and organization.

Unlike physical warfare, conflict in cyberspace does not have a widely agreed-upon set of conventions or norms for regulating conflict. A 2012 academic study, the Tallinn Manual on the International Law Applicable to Cyber Warfare, summarizes the problem:

> *One of the challenges States face in the cyber environment is that the scope and manner of international law's applicability to cyber operations, whether in offence or defence, has remained unsettled since their advent. After all, at the time the current international legal norms (whether customary or treaty-based) emerged, cyber technology was not on the horizon. Consequently, there is a risk that cyber practice may quickly outdistance agreed understandings as to its governing legal structure. The threshold questions are whether the existing law applies to cyber issues at all, and, if so, how.*

Microsoft Approach

Microsoft supports a four-step process for promoting the development and understanding of global cybersecurity norms and practices:

1. Prioritize issues in cybersecurity that require diplomatic engagement from an international legal perspective, and build consensus to incorporate changes caused by technology and innovation into current international laws.

2. Analyze existing cybersecurity best practices and policies at the national, regional, and international levels, and determine where global principles or practices need to be developed. Key areas to explore should include confidence-building measures, responses to security incidents, assessment and mitigation of risk to critical ICT infrastructure, risk management, supply chain security, and protecting core encryption and trust mechanisms of the Internet.

3. Develop a set of cooperative measures for trust, stability, and reliability in cyberspace, with appropriate responsibilities for the public and private sectors, including at the international level.

4. Drive for consensus on the most important issues in cybersecurity, since legal processes take many years to develop and become established both domestically and internationally.

Policy Considerations

Policymakers can facilitate international discussions of cybersecurity norms by promoting five important practices:

- **DEVELOP GLOBALLY HARMONIZED LAWS AND STANDARDS** Given the global and ubiquitous nature of the Internet, developing global cybersecurity laws and standards instead of unique domestic approaches is an important principle. Using common cybersecurity approaches promotes understanding and predictability, and it enables countries to collaborate on problem-solving.

- **REDUCE GLOBAL CYBERSECURITY RISK** As an essential part of diplomacy, governments put a lot of effort into reducing geopolitical risk. Yet, reducing risk is not a well-developed concept under international law or public policy because risks are not usually managed on a global level. The Internet alters that paradigm and brings about the need to discuss risk reduction whenever governments address cybersecurity.

- **BUILD TRUST THROUGH GREATER TRANSPARENCY** Governments can help build trust and increase predictability and stability in cyberspace by practicing greater transparency in their cybersecurity practices.

- **ENCOURAGE COLLABORATION AND INPUT FROM ALL SECTORS** As governments construct cybersecurity practices to address security concerns at the international level, they should seek input from a variety of stakeholders, including the private sector, civil society, and academia.

- **USE PROPORTIONALITY IN DEVELOPING POLICIES AND RESPONSES** Proportionality refers to the well-established principle in international law that policies and responses must be proportional in relation to the need for self-defense. The issue of proportionality is challenging because it is not yet clear how proportionality in cyberspace will be interpreted, and it will likely be analyzed by international tribunals and scholars in conjunction with the principle of "necessity."

National Strategies for Cybersecurity

Key Points

- A national strategy for cybersecurity is a legal and regulatory framework for managing risk and responding to threats posed to the technology infrastructure of a nation.
- Microsoft works closely with governments, enterprises, and customers around the world to assess, manage, and respond to risks, and strongly supports the creation of national strategies for cybersecurity.
- A national strategy for cybersecurity should include risk assessment and management, appropriate security priorities and baselines, threat and vulnerability warnings, security incident management, and promotion of awareness and education.

With societies around the globe growing ever more dependent on information and communications technologies, the imperative of cybersecurity has grown. Cybersecurity issues have developed into significant national-level problems that require government consideration, including the protection of assets, systems, and networks vital to the operation and stability of a nation as well as to the livelihood of its people. Threats against these vital assets target corporations and citizens, and include cybercrime such as identity theft and fraud, politically motivated "hacktivism," and sophisticated economic and military espionage.

Unlike legal systems covering privacy, which have evolved over time to include strong laws aimed at protecting consumer information and preventing online fraud, cybersecurity has not evolved a corresponding legal system over the past decade. In the absence of regulation, information and communications technology (ICT) companies have developed standards and best practices to help establish strong security protections for products and services.

A national strategy for cybersecurity is a legal and regulatory framework for managing risk and responding to threats posed to the ICT infrastructure of a nation. A national strategy is usually created through a complex multi-stakeholder process involving:

GOVERNMENT

ACADEMICS

INDUSTRY

CONSUMERS

NONGOVERNMENTAL ORGANIZATIONS

OTHER

Items that are typically addressed in a national strategy include risk assessment and management, setting appropriate security priorities and baselines, coordinating threat and vulnerability warnings, managing security incidents, and promoting awareness and education.

Microsoft Approach

Microsoft has a unique view of cyberthreats because each month, the company receives threat information from more than one billion systems in more than 100 countries and regions.

Microsoft works with national governments, industry partners, and nonprofit organizations to enhance the security of the Internet. To that end, the company promotes trustworthy plans and policies and helps protect processes that are key to national and economic security as well as public health, safety, and confidence. Microsoft strongly supports governments in creating national strategies for cybersecurity that are based on a principled approach reflecting national priorities.

Policy Considerations

Governments and policymakers can help promote a principled national strategy for cybersecurity by advancing some basic foundational principles:

- **APPLY RISK-BASED STRATEGIES** Assess risk by identifying threats, vulnerabilities, and consequences, then manage it through mitigations, controls, costs, and similar measures.
- **FOCUS ON OUTCOMES INSTEAD OF SPECIFIC REMEDIES** Focus on the desired end state rather than prescribing the means to achieve it, and measure progress towards that end state.
- **PRIORITIZE RESPONSES TO THREATS** Adopt a graduated approach to determining the severity of threats, recognizing that disruption or failure are not equal among critical assets or across critical sectors.
- **SUPPORT BROAD-BASED PRACTICAL SOLUTIONS** Optimize for adoption by the largest possible group of critical assets and implementation across the broadest range of critical sectors.
- **RESPECT PRIVACY AND CIVIL LIBERTIES** Include protections for privacy and civil liberties based upon the Fair Information Practice Principles and other privacy and civil liberties policies, practices, and frameworks.
- **SUPPORT GLOBALLY RELEVANT SOLUTIONS** Integrate international standards to the maximum extent possible, keeping the goal of harmonization in mind.

Collective Defense: Applying Public Health Models to Internet Security

Key Points

- *Malware* (malicious software designed to damage a user's computer, a server, or a network; or to cause harm to computer users by stealing personal or otherwise sensitive information, defrauding, and more) and *botnets* (networks of malware-infected computers controlled by remote attackers) enable cybercrime, costing consumers and businesses billions of dollars each year. In response, a collective defense across the Internet is needed to ensure a systematic approach to dealing with these threats. Improving the health of consumer devices connected to the Internet benefits not only consumers, but the information technology ecosystem as a whole.

- One way to address issues of online security is to apply a model similar to the one society uses to address human illnesses. The public health model of identifying and controlling infectious diseases encompasses a number of concepts that can be applied to Internet security.

Advances in online technology have led to remarkable global development, social change, and an evolution in the way businesses, civil society, and governments work from day to day. Unfortunately, these advances have been accompanied by a rise in online crime, which threatens to undermine the public trust. Today's leaders and decision makers must respond to this new reality with new ideas and solutions, and engage as partners in the public debate on Internet safety, privacy, and accountability. The challenges are substantial and complex:

Cyberthreats have become more widespread, sophisticated, and difficult to characterize, having little in common in terms of origin, path, or impact. This calls for many different responses and solutions worldwide.

Botnets—the most insidious of malware—threaten infrastructure, and in turn endanger financial markets, military institutions, and national security.

Individuals and organizations have a wide variety of choices to help defend their devices against cyberthreats, including antimalware solutions, firewalls, and security updates. However, despite the broad availability of these technologies, they are not always fully deployed. Enterprises spend a lot of time and money to manage risk with well-trained staff and sophisticated systems. Consumers, on the other hand, often lack the expertise and know-how to protect their devices.

One way to address cyberthreats is to model cybersecurity on efforts to address human illnesses. In a public health model, citizens must be aware of basic health risks and be educated on how to avoid them. In schools, for example, students may be required to be vaccinated before admission, warned if other students show symptoms, asked to stay at home if infected, and required to meet specified criteria for readmission.

To improve the security of the Internet, governments and industry could similarly engage in systematic activities to improve and maintain the health of devices connected to the Internet. They could deploy people and technologies to promote preventive measures, detect infected devices, and notify affected users. They could then help users repair malware-infected devices and take additional action to ensure that infected computers do not put other computers at risk.

Some industries and governments have already begun such efforts. For example, the Internet Industry Association of Australia launched its voluntary Internet Service Provider (ISP) Code of Conduct. ISPs that use this system notify consumers who have infected computers and offer them solutions and repair tools. In Germany, the Anti-Botnet-Advisory Centre works in a similar way with local ISPs, which notify and assist consumers whose computers are infected with malware. In Finland, TeliaSonera, an ISP serving 164 million customers, deploys an automated monitoring system to identify infected devices, alert their owners, and quarantine the devices from the network until they are cleaned.

Key Points

- Any effort to promote Internet health and security must be balanced with considerations of the social, legal, and economic issues of privacy, and should be designed not to impact economic activity adversely. An Internet health model works as a collective defense only if it is accepted by society and if people are confident that their privacy will be protected.

Microsoft Approach

Microsoft supports a collective cybersecurity defense similar to a public health model that limits the spread of human illness. Microsoft believes a similar model can be used by governments and IT industry leaders to more methodically prevent, detect, and treat computers infected with malware or botnets.

This model is just a starting point. This vision can become a reality only with the support of consumers, government leaders, and privacy advocates, as well as ISPs and others in the industry. Microsoft works with the IT community to share information on malware and botnets and to help assist affected customers.

Policy Considerations

Industries, governments, and policymakers can help develop and maintain a collective Internet health model by promoting the following practices:

SHARE IDEAS AND COLLABORATE ON COMMON SOLUTIONS Citizens all over the world face more dangers online, and businesses and governments confront substantial cybersecurity issues. To achieve effective and far-reaching goals, all parties must agree to an open exchange of ideas and a sustained commitment to work together to align social, economic, and political innovations and mount a collective defense against cyberthreats.

DEVELOP REGIONALLY SENSITIVE AND LOCALLY SUPPORTED SOLUTIONS As with any international effort, each region has its own unique sensitivities, so solutions must be socially acceptable and meet with local public approval—especially when balancing security and privacy. Global progress on creating a safer online world merits an open exchange of ideas and coordination among industry, government, academics, and all societies worldwide.

Combating Botnets

Key Points

- *Botnets* are networks of compromised computers that are controlled by remote attackers and perform harmful and illegal operations like sending spam, facilitating fraud, and attacking other computers.
- Botnets are of concern to governments and businesses because they can harness large numbers of individual computers to direct an attack against the information technology infrastructure. By working with industry to fight botnets and by passing thoughtful, balanced regulation, governments can help protect their systems and citizens from botnet malware.
- Microsoft aggressively fights botnets by collaborating with governments and others. Microsoft also provides security tools and guidance to businesses, governments, and consumers.

A ***botnet*** is a network of compromised computers that can be illicitly and secretly controlled by an attacker without the knowledge of the computer owners, and then used to perform a variety of illegal actions. Computers in a botnet (also called nodes, bots, robots, or zombies) are usually ordinary computers in homes and offices around the world. A computer becomes a node in a botnet when attackers manage to install malicious software on it, often by using social engineering tactics that trick users into installing it.

The owners of infected computers are usually unaware that their computers are being used for malicious purposes. When a computer has been infected by botnet malware, the botnet owner secretly connects the computer to the botnet and uses it to send spam, host or distribute malware or other illegal files, or attack other computers.

Botnets pose a more dangerous threat than individual hackers to the information technology systems of enterprise and governments because botnets harness large numbers of computers that can be used to direct an attack. The raw computing power of botnets enables them to take down major websites and email servers, as well as other essential parts of critical communications, data, and electronic systems.

Botnets can also pose a threat to IT supply chains. A 2012 Microsoft study found that cybercriminals infiltrated unsecured supply chains using the Nitol botnet, which introduced counterfeit software embedded with malware for the purpose of secretly infecting computers before they were even purchased. Botnets can also provide anonymity to the criminals who control them (known as *botherders*) by enabling them to hide the true source of their attacks behind their widespread network of computers.

Microsoft Approach

Microsoft is determined to help fight cybercrime through:

TECHNOLOGY INNOVATION

LEGAL ACTION

CONSUMER EDUCATION

It supports governments and law enforcement by giving them technical training, investigative and forensic assistance, and the continued development of new technology tools to combat cybercrime.

The Microsoft Active Response for Security (MARS) initiative combines legal and technical acumen to proactively disrupt criminal infrastructure. This includes using private legal action and technology measures to take down botnets, seizing the infrastructure and domains criminals use to control them, and using the information gained in those efforts to better protect the Internet community. Project MARS is a joint effort of the Microsoft Digital Crimes Unit, Microsoft Malware Protection Center, Customer Support Services, and Trustworthy Computing. Recent examples of MARS successes include disruption and remediation of the ZeroAccess, Waledac, Rustock, Kelihos, Zeus, Nitol, and Bamital botnets.

Policy Considerations

Governments and law enforcement can help protect systems and citizens from botnet malware by focusing on several priorities:

- **SUPPORT PUBLIC AND PRIVATE PARTNERSHIPS AND BALANCED REGULATION** Cooperation with authorities is the most effective means for reducing cyberthreats, and balanced regulation is a part of that effort. This includes initiatives like the *Anti-Bot Code of Conduct for Internet Service Providers* recommended by the U.S. Federal Communications Commission. Less onerous restrictions on industry allow for greater innovation and flexibility in implementing responses to cybercrime.

- **ENCOURAGE INTERNATIONAL COOPERATION** Microsoft has joined with industry to encourage countries to adopt and ratify the Council of Europe Convention on Cybercrime, which requires signatories to adopt and update laws and procedures to address online crime.

- **SUPPORT STRONG ENFORCEMENT AND BALANCED REGULATION** The enactment and enforcement of laws to combat botnets and the prosecution of cybercriminals should be a priority. At the same time, it is important that these laws enable innovation and support the adoption of new technology.

Critical Infrastructure Protection

Key Points

- National security and international policy concerns about critical infrastructure have evolved as key systems of public life, health, and safety have become increasingly interconnected and dependent on IT infrastructure.
- The unique security challenges of complex critical infrastructures require an unprecedented response. Technology vendors, governments, businesses, and consumers must work together to innovate, develop, and deploy effective solutions.
- The Microsoft Global Security Strategy and Diplomacy team works with national governments, industry, and nonprofit organizations to strengthen and improve cybersecurity, promote trustworthy plans and policies, and help protect key processes and functions for national and economic security as well as public health, safety, and confidence.

Governments are increasingly focused on the role critical infrastructures play in supporting the overall economy and security of their nations. Critical infrastructures are generally thought of as the key systems (and the services and functions they provide) that, if disrupted, would have a debilitating impact on public health and safety, commerce, or national security.

Advances in software, communications, and IT services have substantially improved and connected these key systems, but their interconnectedness is also a cause for growing concern. Critical infrastructures are attractive targets for criminals. Leaders worldwide are concerned about the security implications of increasingly interrelated global systems that could affect economic stability, climate change, and national security. The potential exists for disruptions of critical infrastructure to cause unprecedented, widespread damage (similar to the recent global financial crisis).

The unique security threats to critical infrastructures pose daunting challenges for those who must predict and manage their outcomes, and they require a united response from governments and businesses. Innovative public-private relationships must develop robust plans to secure and protect critical infrastructures from ever-changing threats and sophisticated attacks. Technology vendors, governments, and businesses must work together to innovate, develop, and deploy effective solutions. Microsoft is dedicated to supporting these relationships and plans to help detect and preempt the sources of threats to critical infrastructure. As part of that commitment, the company formed the Global Security Strategy and Diplomacy team.

Microsoft Approach

The Global Security Strategy and Diplomacy Team is dedicated to enhancing the security and resiliency of critical infrastructures by increasing the trustworthiness of software and IT services, in part through the development of innovative solutions. In addition, the team collaborates with governments and critical infrastructure owners and operators to reduce and manage risks.

Effective efforts to protect critical infrastructure fall within these three areas:

TRUSTWORTHY PLANS AND POLICIES

Clear, effective policies lead to well-defined goals and priorities that help IT professionals secure resources and focus investments on top-priority risks. Microsoft collaborates to develop effective, flexible, and innovative national and global solutions to help secure critical infrastructure.

RESILIENT OPERATIONS

Microsoft helps reduce the impact of disruptions in critical infrastructure by sharing best practices and creating a cohesive front when disruptions occur. Greater resiliency allows IT professionals to manage their environments with greater confidence.

INNOVATIVE INVESTMENTS

Continuous innovation leads to advanced security capabilities. Innovative environments enable IT professionals and organizations to benefit from new thinking; improved products; and better processes, guidance, and training. Microsoft supports collaborative efforts to develop innovative practices, programs, education, and research to develop secure solutions for critical infrastructures.

Policy Considerations

Government and industry policymakers can help in securing and protecting critical infrastructures by supporting the following policies:

- **ENCOURAGE MORE SECURE DEVELOPMENT PRACTICES** Industries should address security and privacy through every phase of product development by using proven, effective processes similar to the Microsoft Security Development Lifecycle.
- **PROVIDE A UNIFIED RESPONSE** Support collaborative relationships and investments that identify assets and manage critical function risks.
- **SHARE INFORMATION AND TEST RESPONSE MECHANISMS** Sharing information and response procedures helps governments and critical infrastructure operators maintain situational awareness and respond quickly to prevent, mitigate, and recover from nationally or globally significant threats.
- **PROMOTE NEXT-GENERATION NETWORK TECHNOLOGIES** Deploy secure cutting-edge solutions to increase communications capability and resiliency.
- **SUPPORT INFORMATION TECHNOLOGY SECURITY RESEARCH** Solve existing problems and prepare for those in the future by strengthening the pipeline of academic and professional knowledge through educating, mentoring, and training future professionals and leaders.

Data Breach Notification

Key Points

- Data breaches put consumers at risk of fraud and identity theft. They also jeopardize consumers' relationships with historically trusted organizations or government infrastructures.

  Microsoft is committed to helping create safer, more trusted computing experiences, and is dedicated to protecting sensitive data and personal information. It recommends a multifaceted approach to data governance that includes policy, people, processes, and technology. The Microsoft approach relies on creating or maintaining more secure infrastructure (as well as identity and access control), protecting information, and auditing and reporting.

- Microsoft supports legislation for data breach notification that includes a risk-based trigger when data containing personal information is acquired by an

In recent years, media reports of data breaches at major public and private institutions have captured both headlines and public attention, especially when they jeopardized the sensitive personal or financial information of millions. Data breaches not only put consumers at risk of fraud and identity theft, but also threaten their trust of reputable organizations and governments.

Governments at all levels are examining the need to revise data breach notification laws. Current laws typically require companies or agencies to notify customers when their personal data has been put at risk or compromised. These laws take one of two forms: an acquisition-based trigger or a risk-based trigger.

Acquisition-based triggers require organizations to notify affected individuals when personal information has been, or can reasonably be assumed to have been, acquired by an unauthorized person. In contrast, *risk-based* triggers require organizations to notify affected individuals when a significant potential risk has been identified.

As policymakers develop new policies governing the notification of data breaches, it is worth noting that in some jurisdictions, organizations are exempt from certain disclosure requirements if their data is encrypted at the time of a security breach. This exemption is a powerful motivator for companies to adopt encryption methods and procedures for protecting sensitive data. In addition, organizations that embrace key concepts of data governance can reduce the risk of data breaches and develop effective plans to address security issues when they do occur.

Microsoft Approach

Microsoft recommends a multifaceted approach to data governance that includes policy, people, processes, and technology. Its approach relies on the following practices:

STRENGTHENED INFRASTRUCTURE with safeguards that help protect systems from malware, intrusions, and unauthorized access to personal information.

IDENTITY AND ACCESS CONTROL with systems that help protect personal information from unauthorized access or use and provide management controls for identity access and provisioning.

Key Points

unauthorized person, and when there is a significant risk of fraud or identity theft. Notification should not be required where the potential of harm is nominal. However, the law should require that affected individuals be notified within a reasonable time period, unless otherwise directed by a law enforcement agency pursuing an investigation.

SECURING SENSITIVE PERSONAL INFORMATION in structured databases and providing safeguards such as encryption for unstructured documents, messages, and records.

AUDITING AND REPORTING on the integrity of systems and data in compliance with business policies.

Policy Considerations

As governments and policymakers develop new regulations for the notification of data breaches, they should focus on the following priorities:

- **COLLABORATE ON SOLUTIONS THAT PROTECT PRIVACY AND INNOVATION** Conflicting laws can complicate compliance across local, state, provincial, or national borders. The wide variance in rules and regulations can impede economic progress and stifle innovation. In countries that have multiple state laws, broad federal preemption should be part of any comprehensive privacy legislation. Policymakers, industry, and organizations should collaborate to develop mutually agreeable solutions that protect both privacy and innovation.

- **CONSIDER DEGREE OF RISK, POTENTIAL HARM, AND TIME** Data breach notification laws should include the following requirements:
  - A risk-based trigger of notification when an unauthorized person acquires data, but only when there is a significant risk of fraud or identity theft.
  - No requirement of notification when the potential harm to the data subject is nominal, such as where information is encrypted or otherwise unintelligible.
  - A requirement to notify those affected within a reasonable time period, unless otherwise directed by law enforcement pursuing an investigation.

- **SUPPORT NOTIFICATION REQUIREMENTS THAT PROVIDE MEANINGFUL INFORMATION** Requirements should support mandatory notification when data breaches occur, but they should be calibrated to provide timely, meaningful information to consumers. Notification mandates with very short time frames run the risk of giving consumers inaccurate or incomplete information. Broad notification requirements that include all data breaches, even where the risk of harm is negligible, run the risk of flooding consumers with notices that will be ignored.

Supply Chain Security

Key Points

- Governments worldwide have concerns about supply chain security, in particular the potential for hostile actors to insert malicious software into information technology products as they move through the supply chain. This could create vulnerabilities in the information and communications technology systems when compromised components are introduced.

- Microsoft employs a four-part strategy to manage the risks to its products and services in the supply chain. This strategy is grounded in identity and access management controls, the Security Development Lifecycle, policies and procedures that monitor the integrity of Microsoft software, and anti-counterfeit measures.

- Governments and businesses need to recognize that supply chain security is a shared problem, and they must work together using risk-based solutions, best practices, and international cooperation.

Some of the more critical information and communications technology systems have become attractive targets for malicious actors who mount increasingly sophisticated attacks. These attacks have the potential to cause widespread damage or disruption to commerce and daily life, or give the attackers unauthorized access to data.

A key area of criminal interest is the supply chain of technology products, which the National Institute for Standards and Technology defines as "the set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers."

The supply chain that is responsible for delivering information and communications technologies is globally distributed. The products themselves can be complex, made of many parts in many different companies all over the world. This raises concerns about the potential for hostile actors to introduce malicious or unwanted functions or counterfeit elements along the way. If products are compromised, they could potentially be used to conduct surveillance or to disrupt or otherwise degrade the trustworthiness of the technology systems of which they will be a part.

Securing such a diverse and global supply chain presents a challenge for governments and businesses. Both need to recognize supply chain security as a shared problem and seek solutions that are built upon best practices, mitigate risks, and draw on international cooperation.

Microsoft Approach

The Microsoft strategy to help mitigate supply-chain risk to its products and services includes the following elements:

IDENTITY AND ACCESS MANAGEMENT CONTROLS

Microsoft uses policies, procedures, and technologies that manage personnel access to Microsoft intellectual property.

SECURITY DEVELOPMENT LIFECYCLE

This is a foundational element for reducing the risk in the development of Microsoft software and for protecting it against the introduction of product vulnerabilities, whether malicious or inadvertent.

SOFTWARE INTEGRITY CONTROLS

Microsoft employs policies, procedures, and technologies to preserve the integrity of its software products, including code signing and checking for malware.

ANTI-COUNTERFEIT MEASURES

To protect customers from the risks of counterfeit software, which could contain vulnerabilities, Microsoft actively identifies counterfeit versions of its software, works to maintain the integrity of its distribution models, and works closely with law enforcement agencies around the world to help reduce piracy.

Microsoft also takes legal and technical action to address criminal efforts to target the supply chain. For example, the Microsoft Digital Crimes Unit works with other Microsoft teams to fight aggressively against botnets.

One such initiative is Project MARS (Microsoft Active Response for Security), which focuses on efforts to disrupt criminal infrastructure. This includes taking legal and technical action to pursue botnets and help undo the damage they cause. In 2012, Project MARS helped take down the Nitol botnet, which infected computers through vulnerabilities in the supply chain.

Policy Considerations

Policymakers who are developing a framework for managing supply-chain risk should base it on the following principles:

- **EMPLOY A RISK-BASED APPROACH** Governments should avoid using simplistic factors, such as a product's country of origin, to assess risk. The global character of many products means that attempts to prohibit products based upon country of origin could result in a broad ban of products. This would lead to weakening open trade and relinquishing the benefits of global innovation. Instead, governments should rely on tested risk-management principles.

- **ENCOURAGE TRANSPARENCY IN PRODUCT DEVELOPMENT** Governments have a right to expect IT companies to provide an appropriate degree of visibility into their business processes as well as the controls that ensure the security of their product development and operations.

  One example of such transparency is the Microsoft Government Security Program, which gives eligible participating governments access to the source code for selected Microsoft products. However, governments also have to appreciate that businesses must protect their trade secrets and other intellectual property.

- **DEVELOP FLEXIBLE STANDARDS** When governments move to adopt standards governing supply chain security, control and mitigation standards need to remain flexible.

- **PROMOTE RECIPROCITY** The development of reciprocal international standards for supply chain security is essential for continuing to realize Internet benefits that rely on the security and integrity of information technology systems.

Microsoft Malware Protection Center

Key Points

- The Microsoft Malware Protection Center (MMPC) antimalware research underlies many Microsoft products and services, enabling the protection of more than one billion computers in 270 countries and regions.
- A worldwide team of researchers ensures that the MMPC can quickly mobilize to identify and mitigate new malware threats within hours of discovery.
- Microsoft collaborates with the security community and other global partners to help create a more secure computing experience and a safer, more trusted Internet environment.
- The MMPC advises customers on the threat landscape by using multiple channels, such as the semi-annual Security Intelligence Report (SIR), the Malware Encyclopedia, and the MMPC website and blogs.

Malware (malicious software) is software that has been designed to damage a user's computer, a server, or a network; or to cause harm to computer users by stealing personal or otherwise sensitive information, defrauding the user through various scams, and other nefarious business. Worms, Trojan horses, viruses, and rogue security software are some of the most prevalent types of malware.

The Microsoft Malware Protection Center (MMPC) is one of the most experienced antimalware organizations in the industry. By building strong partnerships with organizations inside and outside Microsoft as well as continuously analyzing threat data, the MMPC stays agile to combat evolving threats. The mission of the MMPC is to help protect customers and computers by building a comprehensive network of partners dedicated to fighting cybercrime, providing advanced defense through automation and cloud protection services, and quickly responding to malware incidents.

Microsoft Approach

The Microsoft Malware Protection Center combats malware through focused industry collaboration, protection of systems, quick response to threats, and timely and efficient distribution of security information to the general public.

ENGAGE IN PARTNERSHIPS The MMPC recognizes that industry collaboration is the most effective means of eradicating malware and therefore partners with security vendors and corporate entities such as financial institutions, online search companies, and advertising businesses. It also collaborates with Community Emergency Response Teams (CERTs), ISPs, and law enforcement agencies worldwide. The MMPC supports antimalware partners in building a strong and diverse ecosystem to fight malware by using the following strategies:

DIVERSE AND STRATEGIC PARTNERSHIPS The MMPC understands that Microsoft customers are better protected when a coordinated approach to malware eradication is taken. It is committed to building long-lasting strategic partnerships that further diversity, value transfer, and unity among industry partners to fight cybercrime.

KNOWLEDGE SHARING The MMPC publishes and shares world-class security content, malware samples, and telemetry information in an effort to ensure Microsoft customers are better protected.

REAL-WORLD THREAT TESTING The MMPC's commitment to collaboration and sharing telemetry information with antivirus partners and testers enables testing of real-world threats that might affect customers.

HELP PROTECT CUSTOMERS AND SYSTEMS The MMPC team works closely with product engineering teams at Microsoft to help ensure that products have the latest antimalware definitions and can provide accurate and actionable telemetry to enable further research. Malware telemetry enables the MMPC to compare infection rates, patterns, and trends in various locations around the world. MMPC helps protect consumers by providing the following tools and research services:

MALICIOUS SOFTWARE REMOVAL TOOL (MSRT) This free antimalware utility checks computers for infections by specific, prevalent malicious software. When the detection and malware-removal process is complete, the tool displays a report describing the outcome, including which (if any) malware was detected and removed.

RESEARCH AND PROTECTION METRICS MMPC analysts work around the clock to identify, detect, and combat malware. They regularly communicate progress and metrics on coverage of threats, quality of detections, and user experience with customers and partners.

MICROSOFT REAL-TIME PROTECTION SOFTWARE MMPC antimalware research underlies many Microsoft products and services that help protect PCs from malware and other threats.

QUICKLY RESPOND TO MALWARE MMPC research and response efforts focus on real threats that affect customers. Millions of customers have voluntarily opted to share telemetry data on encountered threats, which helps identify and mitigate new malware files within hours of their discovery. By using advanced research, machine learning, and heuristics, and by continuously monitoring for malicious behaviors, the MMPC also provides proactive detection for new threats before even receiving the first sample. A worldwide team of researchers ensures that a response team is always online. It provides malware analysis services through the MMPC website. This site is the central source for malware information, security information, and definition updates. It also provides a place where customers can submit sample malware code for MMPC analysis.

ADVISE CUSTOMERS ON THE THREAT LANDSCAPE AND PROTECTION The MMPC uses multiple channels to distribute malware research and security information to the public:

SECURITY INTELLIGENCE REPORT Microsoft periodically releases the Security Intelligence Report (SIR), a comprehensive evaluation of the evolving threat landscape and trends. Featuring detailed analysis of data from more than a billion computers worldwide who have voluntarily opted to share telemetry data, the SIR helps IT pros make sound risk-management decisions and identify potential adjustments to their organizations' security policies. It also offers case studies from the Microsoft IT group and product teams such as Bing and Internet Explorer.

MALWARE ENCYCLOPEDIA This resource provides detailed analyses of thousands of current threats, including technical information about each threat, how readers can determine whether their computers are infected, and how to recover from or avoid exposure to a threat.

Microsoft Security Intelligence Report

Key Points

- The Microsoft Security Intelligence Report (SIR) offers a comprehensive, up-to-date, and geographically relevant analysis of the cyberthreat landscape of exploits, vulnerabilities, and malware using data from Internet services and more than one billion computers worldwide.
- The Microsoft Trustworthy Computing group is responsible for implementing a long-term collaborative effort to create and deliver more secure, private, and reliable computing experiences through the Security Science initiative, critical infrastructure protection, delivery of secure products, and defense against malware.
- Microsoft believes that industry cooperation with authorities is the most effective means of reducing cyberthreats, and supports balanced regulation as part of that effort.

As the Internet becomes an increasingly integral part of everyday life and the number of people online grows, so too have concerns about online safety—with good reason. Increases in Internet traffic have resulted in dramatic increases in online crime, which has heightened the security concerns of governments and organizations around the world.

Online threats have evolved from petty crimes by attention-seeking hackers to multi-front attacks by sophisticated criminal organizations. Cybercriminals exploit users through email, web browsers, social media, online games, and fake security software. Compromised computers can be used to breach security systems and the data of financial institutions, target political organizations for attacks, and steal people's money or identity—and their sense of security.

As a partner in the global response to online crime, Microsoft provides resources and expertise, including its semi-annual Security Intelligence Report (SIR), to help discover the latest threats. The report offers a comprehensive, up-to-date, and geographically relevant analysis of the cyberthreat landscape of exploits, vulnerabilities, and malware, using data from more than one billion computers worldwide and some of the busiest online services on the Internet. The latest SIR, Volume 15: January–June 2013, is nearly 900 pages of data and analysis with views of 100 locations around the world.

Recent editions of the SIR have shown that cybercriminals are gravitating toward the use of fake software activation keys that contain malware. This emerging social engineering tactic is the number-one threat facing consumers worldwide. The SIR also shows that social engineering and similar attacks can be mitigated through security best practices such as implementing effective technical safeguards.

Microsoft appreciates the scope and changing complexities of online security—and the tremendous value of collaborative effort in the event of an attack to provide support, guidance, and the latest information. To that end, the company continues to promote the global imperative of sharing knowledge with industry leaders, governments, and security organizations.

Microsoft Approach

The Trustworthy Computing group at Microsoft is responsible for implementing a long-term collaborative effort to create and deliver more secure, private, and reliable computing experiences. Areas of the group's focus include the following:

SECURITY SCIENCE Building on a body of research about how systems are attacked and ways to prevent or mitigate those attacks, Security Science is a Microsoft initiative that develops tools and techniques to make attacking systems more difficult. Through Security Science, Microsoft continually monitors threat trends and looks for software vulnerabilities. The company then uses that information to create mitigation tools and techniques that developers can draw on to improve overall security.

PROTECTION OF CRITICAL INFRASTRUCTURE The Trustworthy Computing team engages with governments around the world to help them protect critical infrastructures as well as the safety of their citizens online. The team is committed to sharing its research and innovations to help establish policies that make meaningful improvements to global cybersecurity.

DELIVERY OF SECURE PRODUCTS The Microsoft Security Engineering Center helps protect Microsoft customers by delivering more secure products through the Microsoft Security Development Lifecycle (SDL). The SDL is the industry-leading software security assurance process, which embeds security and privacy through every phase of the development of Microsoft products.

COMBATING MALWARE The Microsoft Malware Protection Center analyzes malicious software and develops solutions that Microsoft uses in its security technologies. When a vulnerability in Microsoft software is discovered, the Microsoft Security Response Center monitors and responds to the incident. It also manages the company's process for releasing security updates and serves as the single point of coordination.

Policy Considerations

A policy framework for providing more secure, private, and reliable online experiences should start with the following priorities:

- **SUPPORT PUBLIC-PRIVATE PARTNERSHIPS AND BALANCED REGULATION** Industry cooperation with authorities is the most effective means of reducing cyberthreats, and balanced regulation is part of that effort. Less onerous restrictions on industry allow for greater innovation and flexibility in developing and implementing responses to cybercrime.

- **ENCOURAGE ADOPTION OF INTERNATIONAL AGREEMENTS** Microsoft has joined with industry partners to encourage countries to adopt the *Convention on Cybercrime* ratified by the Council of Europe, which requires signatories to adopt and update laws and procedures that address online crime.

- **SUPPORT RESEARCH THROUGH GOVERNMENT FUNDING** Government funding of basic security research can help improve the security of online systems and ultimately lead to a safer and more reliable online experience for consumers.

Microsoft Security Development Lifecycle

Key Points

- The Microsoft Security Development Lifecycle (SDL) is a security assurance process for software development; it builds security into every phase of software development and provides defense-in-depth guidance and protection.

- The SDL is a hands-on set of procedures involving testers, developers, program managers, and architects working with product security teams across the company. Its security innovations are integrated into Microsoft Office, the Windows operating system, Microsoft SQL Server, and many other Microsoft products and services.

- The SDL is continuously evolving and improving. It is updated to take advantage of newly developed defensive techniques in security science and in anticipation of emerging threats.

Today's cybersecurity threats are ever-changing. They require an ongoing multifaceted response from the information technology industry for development solutions that optimize software security and provide for safer computing experiences for people around the world.

The Microsoft Security Development Lifecycle (SDL) is the company's security assurance process for software development that introduces security and privacy at every step of the way. It offers a holistic and practical approach to addressing evolving security threats and increasingly sophisticated cybercrime.

Microsoft developed the SDL process in 2004 as part of a defense-in-depth approach to security, and it celebrates its 10-year anniversary in 2014. It was created to reduce the number of vulnerabilities in Microsoft software and to give users high-quality, meticulously engineered, rigorously tested software that better defends against malicious attacks. Microsoft engineers and security experts realized that performing security activities as part of a repeatable process results in greater security gains and return on investment, and creates a more secure Internet environment. Using the SDL helps developers create software that has fewer, less severe vulnerabilities.

ISO/IEC 2703410 is a six-part standard created by Subcommittee SC27 of the Joint Technical Committee of the International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27034-1 helps guide and measure application security programs instead of replacing them. In Annex A of the standard publication, the first case study presented is a detailed mapping of Microsoft SDL to ISO/IEC 27034-1. The standard's authors tagged specific elements of the SDL as belonging to specific containers within the Organization Normative Framework, as depicted in the following figure. Because of the work already done to map Microsoft SDL with ISO/IEC 27034-1, use of the SDL for an application security program lends itself to being evaluated by ISO/IEC 27034-1 principles.

TRAINING

- Core Security Training

REQUIREMENTS

- Establish Security Requirements
- Create Quality Gates/Bug Bars
- Security and Privacy Risk Assessment

DESIGN

- Establish Design Requirements
- Analyze Attack Surface
- Threat Modeling

IMPLEMENTATION

- Use Approved Tools
- Deprecate Unsafe Functions
- Static Analysis

VERIFICATION

- Dynamic Analysis
- Fuzz Testing
- Attack Surface Review

RELEASE

- Incident Response Plan
- Final Security Review
- Release Archive

RESPONSE

- Execute Incident Response Plan

Key Points

- Microsoft shares the SDL with the software industry. It has been adopted (sometimes in a modified form) by a variety of software and hardware vendors, government agencies, and software development organizations.

Microsoft Approach

Using the SDL is a mandatory practice for product development at Microsoft. As shown in the previous figure, it includes a series of systematic security- and privacy-focused activities throughout the software development lifecycle—from technical training for engineers to processes for emergency responses after deployment.

Software development is an evolving process, and so is the SDL. While it's impossible to completely prevent all vulnerabilities during software development, when they do emerge, Microsoft engineers perform root-cause analysis to understand the problem. They then identify corrective actions and incorporate that knowledge into the next version of the SDL.

Implementing the SDL has led to measurable improvements in the security and privacy of Microsoft products.

When it comes to security, Microsoft believes in a collective approach that involves the entire IT community so that the company shares security expertise, process guidance, and technology with developer and IT professional communities worldwide. As of 2013, IT professionals downloaded Microsoft SDL guidance, white papers, and tools and resources more than one million times.

Policy Considerations

Government and industry policymakers can encourage software development practices that result in safer computing experiences for people around the world by advancing the following principles:

- **SUPPORT ADOPTION OF INDUSTRY-WIDE SDL DEVELOPMENT METHODS** The SDL Chronicles document how the Microsoft Security Development Lifecycle has helped public and private organizations change their engineering cultures and develop more secure software. Key industry leaders, including Cisco and Adobe, have based their security development methods on the Microsoft SDL.

- **ENCOURAGE INNOVATION AND NEW TECHNOLOGIES** Any government approach to addressing the problems of information security should also protect innovation and ensure the continued adoption of new technologies. Government and industry can work together to establish appropriate principles that strike the right balance between regulation and innovation.

Microsoft Security Response Center

Key Points

- The Microsoft Security Response Center (MSRC) serves as a single point of security coordination and communications, and is led by some of the world's most experienced experts. The MSRC identifies, monitors, resolves, and responds to security incidents, including vulnerabilities in Microsoft software. It also manages and publishes the monthly security updates, Security Advisories, and the Security Update Guide.

- Microsoft collaborates with the security community and other global partners to help create a more secure computing experience and a safer, more trusted Internet environment through programs such as Microsoft Active Protections Program (MAPP), the BlueHat security briefings, the Microsoft Bounty Programs, and by participating in industry conferences worldwide.

Computer security is an ongoing, ever-changing challenge. Threats have become more complex and widespread as cybercriminals continue to develop sophisticated new ways to attack both large interconnected systems and individual customers.

The Microsoft Security Response Center (MSRC), part of the Trustworthy Computing Group, was created to help keep pace with evolving threats and better protect customers against malicious attacks using a multi-pronged approach. Led by some of the world's most experienced security experts, the MSRC serves as the company's single point of coordination and communication on security threats.

Microsoft Approach

Microsoft is committed to protecting consumers by delivering timely and effective responses to threats, collaborating with industry partners, and continually advancing innovation.

DELIVER WORLD-CLASS SECURITY RESPONSE For more than 10 years, the MSRC has been distributing timely security updates and authoritative security guidance to customers, industry partners, and the security community.

SECURITY SOFTWARE UPDATES October 2013 marked the 10-year anniversary of Update Tuesdays, the process Microsoft uses to provide the latest security updates for all of its products. Throughout this process, MSRC case managers balance scope, schedule, and priorities while accounting for code completeness and quality. MSRC experts write the accompanying security bulletins, which are translated into multiple languages and machine-readable formats (CVRF), then published on the second Tuesday of each month.

MICROSOFT SECURITY ADVISORIES, introduced in 2005, are a supplement to the security bulletins that addresses security changes that may not require a bulletin, but that may still affect customers' overall security.

THE MICROSOFT SECURITY UPDATE GUIDE helps IT professionals better understand and maximize Microsoft security update release information, processes, and tools.

MICROSOFT BOUNTY PROGRAM is an award program that pays researchers who find mitigation bypass techniques in the latest Microsoft platform and defensive ideas that work against these techniques.

Key Points

Microsoft is committed to advancing the quality and innovation of software security updates by leading initiatives such as the Microsoft Exploitability Index, Security Update Validation Program (SUVP) and the Enhanced Mitigation Experience Toolkit (EMET).

ACTIVELY COLLABORATE WITH SECURITY PARTNERS The MSRC collaborates with the security community and industry partners to help Microsoft advance and improve security for customers and the broader security ecosystem

MICROSOFT ACTIVE PROTECTIONS PROGRAM (MAPP) offers approved security software providers and incident responders' information about vulnerabilities and threats in advance of the Microsoft monthly security update. This advance warning gives these MAPP partners more time to build protections against the vulnerability so they can give their customers updated protections faster.

BLUEHAT SECURITY BRIEFINGS are invitation-only conferences aimed at advancing the security of Microsoft products. Microsoft security professionals and outside researchers come together to share ideas and expertise about threats to global security.

CONFERENCE SPONSORSHIPS support and advance the research community. The MSRC engages with the security community by co-sponsoring or attending over 40 security conferences worldwide each year.

MICROSOFT VULNERABILITY RESEARCH (MSVR) is a program through which Microsoft shares its collective experience and best practices in dealing with vulnerabilities within the security community. The goal is to foster positive change, which will ultimately improve the security ecosystem.

ADVANCE INNOVATION AND QUALITY The MSRC has a commitment to excellence, innovation, and quality that helps Microsoft continually improve and evolve in the security landscape.

THE MICROSOFT EXPLOITABILITY INDEX (EI) was launched in 2008 to help customers evaluate risk by providing information on the likelihood that a vulnerability addressed in a Microsoft security update will be exploited within the first 30 days of the update's release.

THE MICROSOFT SECURITY UPDATE VALIDATION PROGRAM (SUVP) provides a small number of dedicated, external participants with limited and very controlled access to security updates. The sole purpose of this program is to test for application compatibility, stability, and reliability in simulated production environments. The end result of this program is higher-quality updates for customers, which helps ensure more timely and effective deployment of updates.

ENHANCED MITIGATION EXPERIENCE TOOLKIT (EMET) helps prevent attackers from gaining access to computers. EMET anticipates the most common actions and techniques adversaries might use in compromising a computer. EMET helps protect computer systems even before new and undiscovered threats are formally addressed by security updates and antimalware software.

Resources

GENERAL

Microsoft Trustworthy Computing: **www.microsoft.com/twc**

Microsoft Safety and Security Center: **www.microsoft.com/security**

Microsoft Privacy Policies and Initiatives: **www.microsoft.com/privacy**

Microsoft Security Essentials: **www.microsoft.com/security_essentials**

Microsoft Security Software:
www.microsoft.com/security/portal/mmpc/products/default.aspx

CYBERSECURITY

Rethinking the Cyber Threat: A Framework and Path Forward (PDF, 537 KB):
aka.ms/cyber-threat

Malicious Software Crimes: **aka.ms/DCU-economic-crime**

CYBERSECURITY NORMS

Cybersecurity and Cyberwarfare 2011: Preliminary Assessment of National Doctrine and Organization:
aka.ms/CSIS-CyberConflict

Cybersecurity Norms and the Public Private Partnership: Promoting Trust and Security in Cyberspace:
aka.ms/norms-public-private

Cybersecurity Norms for a Secure Cyber-Future: **aka.ms/Secure-cyber-future**

Developments in the Field of Information and Telecommunication in the Context of International Security (UN First Committee): **aka.ms/UN-cyber-security**

NATIONAL STRATEGIES FOR CYBERSECURITY

Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation: **aka.ms/National-Strategy**

COLLECTIVE DEFENSE: APPLYING PUBLIC HEALTH MODELS TO INTERNET SECURITY

Microsoft End to End Trust—Internet Health: **aka.ms/internet-health**

The Internet Health Model for Cybersecurity. EastWest Institute, 2012:
www.issuu.com/ewipublications/docs/internethealth/1?e=0/5313787

COMBATING BOTNETS

Microsoft Active Response for Security (MARS):
www.microsoft.com/government/ww/safety-defense/initiatives/Pages/dcu-economic-crime.aspx

Microsoft Digitial Crimes Unit (DCU): **www.microsoft.com/dcu**

SUPPLY CHAIN SECURITY

Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust:
aka.ms/supply-chain-risk

Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity:
aka.ms/Trusted-Supply-Chain

MICROSOFT MALWARE PROTECTION CENTER

Microsoft Malware Protection Center: **www.microsoft.com/mmpc**

MMPC blog: **blogs.technet.com/mmpc**

Malware Encyclopedia: **www.microsoft.com/security/portal/threat/Threats.aspx**

MICROSOFT SECURITY INTELLIGENCE REPORT

Microsoft Security Intelligence Report: **www.microsoft.com/sir**

Microsoft Security Engineering Center: **www.microsoft.com/security/msec.aspx**

MICROSOFT SECURITY DEVELOPMENT LIFECYCLE

Life in the Digital Crosshairs: **www.sdlstory.com**

Microsoft Security Development Lifecycle: **www.microsoft.com/sdl**

The SDL Chronicles: **aka.ms/SDL-Chronicles**

Software Assurance Forum for Excellence in Code (SAFECode): **www.safecode.org**

MICROSOFT SECURITY RESPONSE CENTER

Microsoft Security Response Center: **www.microsoft.com/msrc**

MSRC blog: **blogs.technet.com/msrc**

MSRC Twitter: **@msftsecresponse**

Microsoft Active Protections Program (MAPP): **aka.ms/ms-mapp**

Microsoft Exploitability Index: **aka.ms/Exploitability-Index**

GLOBAL INITIATIVES AND PARTNERSHIPS

Microsoft Global Security Strategy and Diplomacy: **www.microsoft.com/cybersecurity**

Convention on Cybercrime: **aka.ms/Convention-on-Cybercrime**

Tallinn Manual on the International Law Applicable to Cyber Warfare: **aka.ms/Tallinn-Manual**

The Industry Consortium for Advancement of Security on the Internet: **www.icasi.orga**

Microsoft

Privacy

Building Global Trust Online, 4th Edition

Microsoft Perspectives for Policymakers

Our Commitment to Privacy

Microsoft is committed to earning customer trust by demonstrating accountability and an inherent respect for privacy. We must earn customer trust by being as transparent as possible about the people, policies, and processes we have in place to protect privacy.

Our approach to privacy[1]

We strive to use people's data responsibly, be transparent about our privacy practices & offer meaningful privacy choices

Microsoft conducts privacy reviews of new features, products, devices and services before release

The Microsoft Corporate Privacy Policy comprises 10 privacy principles to protect and appropriately use customer information

CONSUMERS

microsoft.com/yourprivacy provides guidance on how consumers can better protect their information online

ENTERPRISE

The Office 365 Trust Center, the Windows Azure Trust Center, and Dynamics CRM Online Trust Center and the Intune Trust Center describe how Microsoft cloud services help protect information privacy

The Microsoft Privacy Guidelines for Developing Software Products and Services is a public version of our internal privacy protection guidelines for our products and services

POLICY[2]

Microsoft works with governments, businesses, technology leaders, and civil society to:

Advise on legislative proposals

Help ensure interoperability of laws across jurisdictions

Develop responsible privacy practices

Strengthen self-regulatory mechanisms that support privacy and data protection

Read on to learn more about how Microsoft is innovating in privacy protection in support of consumers, enterprises, and government policy

[1]www.microsoft.com/en-us/twc/privacy/practices.aspx | [2]www.microsoft.com/en-us/twc/privacy/policy-activity.aspx

Privacy

Key Points

- Consumers expect strong privacy protections to be built into their products and services, and have high expectations about how companies collect, use, and store their information. Public trust depends on people knowing that their privacy will be protected and that their personal information will be used appropriately.

- Microsoft has a longstanding commitment to privacy. The company takes steps to responsibly manage customer information, promote transparency, and offer meaningful privacy choices. Microsoft has more than 40 employees working full time on privacy, and several hundred others worldwide focused on privacy as part of their jobs.

- Microsoft supports privacy legislation that facilitates the free flow of information, builds trust with consumers, and encourages innovation. Because data increasingly flows across geopolitical borders, the company favors interoperability of privacy regulations, policies, and standards.

The digital economy has changed the world in profound and exciting ways. At the same time, public concern about privacy, including the collection and use of personal information as well as widely publicized data breaches, threatens to erode public confidence in digital commerce and the Internet.

Consumers expect strong privacy protections to be built into their products and services and have high expectations about how companies collect, use, and store their information. Public trust depends on people knowing that their privacy will be protected and that their personal information will be used appropriately. If companies fail to meet these standards, people may be less inclined to use online technologies, and both industry and consumers will suffer.

Microsoft Approach

Microsoft has a longstanding commitment to privacy and takes steps to responsibly manage customer information, promote transparency, and offer meaningful privacy choices. The company's approach includes the following priorities:

PROMOTING PRIVACY FUNDAMENTALS

Microsoft understands that respect for privacy is essential to a computing environment that is trustworthy. Microsoft employs more than 40 full-time privacy professionals and several hundred more employees worldwide who are responsible for ensuring that privacy policies, procedures, and technologies are applied company-wide.

PROTECTING USER INFORMATION

Microsoft believes that people should have control over their personal information and that organizations should be responsible and accountable for how they collect, use, and protect this information. Microsoft privacy principles and privacy statements provide clearly worded explanations of what information Microsoft collects, why, and how it is used. They also offer guidance on how consumers can manage the information they provide to Microsoft.

PROVIDING POLICY LEADERSHIP AND COLLABORATION

Microsoft works with governments, consumer advocates, businesses, and technology industry leaders to advise on legislative proposals, help create interoperable laws across jurisdictions, develop responsible privacy practices, and strengthen self-regulatory mechanisms that support greater protections for individuals and their personal information. The company's public policy efforts include advocating for new and updated regulatory approaches to promoting a safer, more open cloud computing environment, and baseline federal privacy legislation. Microsoft also works with law enforcement agencies and consumer and advocacy organizations around the world to combat fraud, spam, spyware, and other threats to privacy online.

Policy Considerations

Policymakers in government and industry can help protect consumers' privacy and ensure that personal information is used appropriately by focusing on several priorities:

- **SUPPORT BALANCED, GLOBALLY INTEROPERABLE REGULATIONS AND STANDARDS** Privacy legislation should encourage innovation, facilitate the free flow of information, and help build trust with consumers. Because data exchanges are increasingly global, there should be greater interoperability of privacy regulations, policies, and standards worldwide.

- **ENCOURAGE INNOVATION AND NEW TECHNOLOGY** As governments act to address issues associated with emerging technologies and online services, they should not stifle innovation and the adoption of technology in the process. Government and industry can work together to establish appropriate and balanced principles that can be globally interoperable.

- **SUPPORT A "DATA USE" MODEL FOR PRIVACY REGULATIONS** The way data is used, rather than how it is collected, might be a more effective premise for protecting data and meeting privacy obligations related to that data. Instead of relying strictly on notice and consent, policymakers should support a model that focuses on data use.

Baseline Privacy Legislation

Key Points

- In countries (like the United States) that have a patchwork of local and national privacy laws, policymakers should align these widely varied privacy requirements through clear, cohesive, and comprehensive national legislation.
- Microsoft has led the call for comprehensive federal privacy legislation in the United States since 2005. The company advocates national legislation that will give people greater control over the collection, use, and disclosure of their information and greater assurances about the security of their information.
- Microsoft believes that baseline privacy legislation should apply to both online and offline computing and should include requirements for transparency, consumer control, and security. Privacy legislation should create legal certainty by preempting local laws that are inconsistent with national policy. It should also promote accountability by ensuring that all businesses are using, storing, and sharing

Many countries have comprehensive privacy laws that govern how personal information is collected, used, and shared, and data protection authorities typically enforce those laws. In the United States, by contrast, privacy is governed through a combination of local and national laws that apply to specific industry sectors. This fragmented approach has led to a growing number of differing local and national laws, creating an environment of uncertainty for organizations and inconsistent protections for consumers.

Baseline national privacy legislation would help create legal certainty by preempting state or other local laws that are inconsistent with national policy. It could promote both accountability and innovation by helping ensure that all businesses are using, storing, and sharing data in responsible ways, while still encouraging companies to compete on the basis of more robust privacy practices.

Government and industry can work together to develop effective, consistent, and constructive privacy protection frameworks that streamline an increasingly complex set of laws governing privacy and data protection. Greater clarity and alignment of regulatory efforts can improve transparency, security, and consistency—and give consumers greater control over their personal information.

Microsoft has long advocated for the development and implementation of comprehensive national privacy legislation. The company also works with various regional stakeholders to advance the Asia-Pacific Economic Cooperation (APEC) privacy framework.

Microsoft Approach

The longstanding commitment Microsoft has made to privacy includes principles, policies, and procedures for building privacy protections into its products and services—from development through deployment and operation. Microsoft has been a leading advocate for comprehensive federal privacy legislation in the United States since 2005. The company believes that federal legislation is necessary to give consumers greater predictability regarding the collection, use, and disclosure of personal information, as well as greater confidence in their online and offline transactions.

Key Points

commercial data in responsible ways.

- Privacy legislation cannot be expected to solve all privacy challenges by itself. To achieve the broadest protection for consumers, such legislation should be paired with industry self-regulation and best practices, technology solutions, and consumer education.

Microsoft shares information and ideas about many of the privacy-related legislative proposals that are taking shape around the world. The company's efforts include providing comments and feedback to the U.S. Federal Trade Commission (FTC) on the preliminary staff report on consumer privacy, and on supplemental proposed revisions to the rule implementing the Children's Online Privacy Protection Act (COPPA). Microsoft also participated in the consultation process for the European Union Data Protection Directive, and it supported the development of the Asia-Pacific Economic Cooperation Privacy Framework. Further, Microsoft submitted comments in response to The White House Office of Science and Technology Policy's Request for Information regarding big data, and supported strengthening but adapting privacy law to enable the collection and use of data in a big data environment while preserving privacy, as well as adoption of baseline federal privacy law.

Policy Considerations

Policymakers can help provide consumers with greater control over the collection, use, and disclosure of their information by focusing on these priorities:

SUPPORT COMPREHENSIVE PRIVACY LEGISLATION Baseline federal privacy legislation should apply both online and offline, and it should include requirements for transparency, consumer control, and security. Legislation should create legal certainty by preempting state or local laws that are inconsistent with federal requirements. It should also promote accountability by ensuring that all businesses use, store, and share data responsibly, while encouraging competition on the basis of more robust privacy practices.

PROMOTE INDUSTRY SELF-REGULATION, BEST PRACTICES, AND CONSUMER EDUCATION Privacy legislation is not a complete solution. While comprehensive legislation can and should create flexible, baseline standards, public policy is unlikely to keep pace with evolving technologies and business models. The most effective approach to protecting consumer privacy will be to pair baseline legislation with industry self-regulation and best practices, technology solutions, and consumer education.

REWARD SELF-REGULATION AND VOLUNTARY COMPLIANCE Privacy legislation should include safe harbors for companies that comply with government-approved self-regulatory programs. Voluntary codes of conduct, which should be developed through open, multi-stakeholder processes, can build upon baseline statutory requirements—and therefore better address and adapt to emerging technologies and rapidly evolving business models.

Future Privacy Models

Key Points

- In light of the burden to consumers posed by the increasingly complex uses and reuses of their data, the current data protection model of notice and consent as the primary tool for data privacy should be reconsidered.
- Decision-makers should explore new models that retain the value of notice and consent where appropriate while shifting the focus of data protection to the use of information by accountable organizations.
- Microsoft encourages the adoption of privacy models based on use and organizational accountability, with corresponding legislation and enforcement capability that supports this approach.

Traditionally, data privacy in many parts of the world has been based upon the concepts outlined by the Fair Information Practice Principles, which rely upon protection mechanisms like notice and consent. This model typically requires an organization to give notice to individuals, often via a privacy statement, describing what information will be collected and how it will be used. Consumers give their consent by agreeing to the privacy statement or continuing to engage with the service. The organization commits not to use data in a manner inconsistent with the disclosures and consumers' consent.

However, in the modern information economy, the massive aggregation of digital information (sometimes referred to as big data) and increasing use of cloud computing are creating highly complicated flows of data that significantly strain the notice-and-consent model in at least four significant ways:

1. COMPLEX MANAGEMENT Choices regarding the collection of an individual's data and its use have become so numerous and detailed they are difficult for most individuals to interpret and manage.

2. CHANGING RELATIONSHIPS The model assumes an interactive relationship between the individual and the entity collecting and using the data—a relationship that increasingly may not actually exist with the proliferation of information sensors.

3. FUTURE USES OF DATA The true value of data may not be understood at the time of collection, and future uses that have significant individual and societal benefit may be lost if privacy models focus solely on enumerating potential uses at the time of the collection of data.

4. DATA PROCESSING AND ANALYSIS Increasingly large amounts of data will be created by entities (rather than amassed through collection alone) through analysis and data processing, further complicating the construct of notice and consent at the point of data collection.

There is a growing focus among privacy experts on the need for evolved data protection models, as the creation and use of data continues to grow. Under the current model, much of the responsibility for privacy protection rests with individuals, who are expected to read and make informed decisions based on the numerous lengthy, complex privacy statements and disclosures of online service providers. It is absolutely essential that organizations continue to be transparent about their data collection and use practices. However, if protection of personal privacy is to be meaningful, new models should be explored that retain the value of notice and consent in more appropriate ways while shifting the focus of data protection to the use of information by accountable organizations.

An additional challenge in our current data protection model relates to the specification of data use at the time of its collection. Today's technology-enabled data analysis and use are providing rich value-added scenarios and services to consumers, businesses, and society in general. However, there may be the potential to unlock additional value in data that was not contemplated at the time of collection.

Shifting the focus from a consent model to a data use model does not mean eliminating the concept of consent. Rather, a model that is more focused on use adds tools to the data protection arsenal, which can help cover gaps that are currently difficult to govern. Individual participation and consent remain critical parts of the privacy model and will become more important when individuals are confronted with data use or collection requests that are outside societal norms.

Microsoft Approach

Microsoft actively supports the idea that society must evolve its current data protection model and address its shortcomings by focusing less on the collection of data and more on the use of data. This does not mean collection limitation is unimportant—rather that it's not something societies can depend on as heavily for privacy protection in today's data-driven society.

Microsoft believes in the need for a greater focus on organizational accountability for responsible use of information, accomplished through formal assessment of the risks to individuals. The company recognizes the need for principles governing data usage that give individuals greater control over their data and provide greater transparency into how companies manage and use it.

Collectively, societies should focus on having the right privacy models in place that protect individuals' privacy needs while enabling accountable organizations to take advantage of the economic and social value of data use in a world of big data.

Policy Considerations

As societies work to evolve today's privacy models, policymakers should explore the following policy and regulatory considerations:

- **SUPPORT PRIVACY MODELS BASED ON DATA USE** Legislation should support privacy models that incorporate data use based on principles. A model based on data use can exist with an evolved set of Fair Information Practices as well as appropriate, relevant notice and consent in the privacy process. It also in no way diminishes the requirement that information be collected in a fair and lawful manner.

- **PROVIDE ADEQUATE ENFORCEMENT AND OVERSIGHT** Enforcement models should be resourced to tackle the oversight challenges that are associated with embracing greater organizational accountability for data use.

- **ENCOURAGE INNOVATION AND PUBLIC-PRIVATE COLLABORATION** As governments act to address issues associated with emerging technologies and online services, they should not stifle innovation and technology adoption in the process. Government and industry can work together to envision and identify the future of privacy models.

Microsoft Privacy Statements

Key Points

- Improvements to Microsoft online privacy statements enhance their design and functionality to more effectively layer important information and make that information easier to locate and use.
- Migration to the new privacy statement format will be gradual but steady. Bing and Microsoft.com were the first to adopt it, followed by Xbox; other Microsoft products and services will follow over time.
- Microsoft remains steadfast in its longstanding commitment to protecting customer data and continues to uphold its privacy policies and practices. There are no material changes to Microsoft data collection and use practices as a result of the redesign.

Privacy statements describe the information a company collects and how that information is used and shared. However, the increasingly complex nature of global data flows, along with new privacy regulations, has led to privacy statements that are often lengthy and difficult to read. In addition, many organizations have dozens (even hundreds) of different online resources or services, which can lead to multiple, overlapping privacy statements.

The challenge for companies is to create meaningful privacy statements that convey the most important elements in a clear and understandable way, and offer easy access to additional details for those seeking more complete information.

One way to accomplish these goals is through a layered privacy notice. A layered privacy notice lists the most important features of the privacy statement. After each feature, viewers are offered a link to more detail. In 2006, Microsoft was one of the first companies to implement a layered privacy statement.

In July 2012, Microsoft updated its online privacy statements to enhance their functionality and provide greater consistency across Microsoft products and services. Migration to the new format is ongoing, with Bing and Microsoft.com (illustrated in the following figure) being the first to adopt the new format, followed by Xbox in October 2012, and MSN in December 2013.

Microsoft Approach

By providing a new format and design of its privacy statements, Microsoft aims to accomplish the following:

IMPROVED CONSISTENCY AND AVAILABILITY Enhance functionality by enabling more effective layering of important information and creating a consistently accessible structure across many Microsoft products.

EASE OF USE Make it easier and more efficient for customers to discover and go directly to the privacy statement for the specific product or service they are using.

BETTER ORGANIZATION Include clearly defined subsections specific to different types of data collection and use, such as advertising and cookies, how information is collected and used, why it's shared, how users can access their information, and privacy (especially as it applies to children).

Microsoft remains steadfast in its longstanding commitment to protect customer data and continues to uphold its privacy policies and practices. There are no material changes to Microsoft data collection and use practices resulting from this redesign.

Policy Considerations

Government and industry policymakers alike can help ensure that privacy notices are transparent, discoverable, and easy to understand by focusing on the following priorities:

- **PROVIDE FLEXIBLE LEGISLATION THAT ALLOWS FOR INNOVATION** Flexible legislative frameworks will help to ensure both that consumers have robust privacy protections and that businesses are able to develop and offer innovative products and services. Legislation that follows these criteria will also be more resilient to technological and business change, helping to protect customer data not only today, but in the years to come.

- **AVOID "ONE-SIZE-FITS-ALL" MANDATES** Although governments have an important role in encouraging companies to provide clear and understandable privacy statements for consumers, they should avoid mandates that could lead to "one-size-fits-all" privacy policies.

- **SUPPORT ADAPTABILITY IN INDUSTRY POLICIES AND PRACTICES** People's privacy expectations vary depending on the nature of their relationship with a specific company. Any legislation, therefore, should permit businesses to adapt their policies and practices to the context in which personal information is used and shared.

Privacy Accountability

Key Points

- Under the principle of accountability for data privacy, an organization is responsible for understanding the risks that are inherent in processing individuals' personal or sensitive data; for creating policies, tools, and processes to mitigate those risks; and for ensuring that internal privacy controls safeguard personal data.

- Accountability for data privacy is a key Microsoft principle that helps determine how the company and its vendors manage personal data. Each Microsoft business unit is responsible for adopting procedures to help uphold the company's commitment to protecting personal data.

- Microsoft supports an accountability-based approach to data use and data transfers across international borders. Under an accountability regime, data could be used for activities based on accepted societal norms and be transferred across borders without restriction as long as the data exporter remains accountable for protecting the data regardless of its geographic location.

Accountability is a long-established principle of privacy and data protection. It was first set by the Organization for Economic Co-operation and Development (OECD) in the early 1980s. The intent of accountability can be found in the laws of the European Union (EU) and EU member states and is outlined more explicitly in the Canadian Privacy Law (PIPEDA) and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

Accountability requires companies that use and store data to analyze and understand the related privacy risks for individuals, and take necessary and appropriate steps to mitigate those risks. Accountability calls upon organizations to implement programs that align with data protection principles, take responsibility for the safe and appropriate use and storage of data (regardless of its location), and be able to explain how its programs provide the required protections for individuals' data.

The importance of accountability for data protection and privacy has never been greater. Technical innovations related to data collection, analysis, and processing; greater access and flow of data worldwide; and the development of powerful analytic tools have created a situation where more usable data exists than ever before. This new world of available, interconnected data requires meaningful privacy safeguards that can address the size of the challenge.

Accountability for data privacy has experienced a recent resurgence in privacy policy circles worldwide. The privacy community is evaluating how to evolve current privacy models and principles to achieve meaningful privacy protections in a world of big data. The widespread adoption of a principle of accountability offers many potential benefits; it can help facilitate the flow of data across international borders and support cloud computing by requiring that businesses take responsibility for the management of information, regardless of how it is collected or used.

Microsoft Approach

A key Microsoft privacy principle is that of accountability in handling its customers' personal data within the company and with its vendors. Each Microsoft business unit is accountable for implementing procedures to help safeguard data and for assigning responsibilities for privacy protection to specific staff members.

Microsoft works with policymakers and other stakeholders to consider how organizations can implement and advance accountability, and whether (and how) third-party accountability agents and other validation programs might play an appropriate and proportionate role in this evolving paradigm.

Policy Considerations

Policymakers and other stakeholders can support the principle of accountability for data privacy by focusing on several priorities:

- **SUPPORT AN ACCOUNTABILITY-BASED APPROACH TO DATA PRIVACY** Such an approach would hold the data collector accountable for its uses and transfers of personal information. An accountable organization incorporates privacy protections in its technology systems and data management processes. The organization provides clear privacy notices that state what steps are being taken to minimize privacy risks and offers appropriate choices for individuals regarding data collection and usage.

- **LIMIT RESTRICTIONS ON INTERNATIONAL DATA TRANSFER** An accountability regime must permit data to be transferred across international borders without restriction as long as the data exporter remains accountable for protecting the data regardless of where it resides.

- **SUPPORT INNOVATION AND FLEXIBILITY WHILE PROTECTING CONSUMER PRIVACY** Policymakers and other stakeholders should carefully consider how the accountability model might work within legal regimes so as to better protect consumer privacy—and permit organizations to use data in responsible and flexible ways to support innovation.

- **AVOID IMPOSING DIFFICULT VALIDATION REQUIREMENTS** Accountability should not require burdensome external validation mechanisms. For instance, imposing third-party audits or certification schemes can be onerous, expensive, and disproportionate to the potential privacy risks.

Privacy by Design at Microsoft

Key Points

- The longstanding Microsoft commitment to privacy includes tools, technologies, people, processes, and procedures for embedding privacy protections in its products and services—from development through deployment and operation.
- Microsoft employs more than 40 people who work full time on privacy, and hundreds of other employees worldwide focus on privacy as part of their jobs.
- Microsoft supports privacy legislation initiatives that facilitate the free flow of information, build trust, and encourage innovation. Because data increasingly flows across geopolitical borders, the company favors greater interoperability of privacy regulations, policies, and standards worldwide.

Privacy by Design has become a popular term in the privacy community, but it means different things to different people. At Microsoft, Privacy by Design describes not only how the company builds products, but also how it operates its services and conducts business as an accountable technology leader. Microsoft believes that all companies that operate online should adopt privacy practices that build trust with the customers who use their products and services.

Microsoft addresses Privacy by Design with principles, policies, and procedures to establish privacy-specific design objectives for its software products and online services at the outset of development. The company continues to address privacy and data security considerations throughout the product life cycle and uses internal processes to track compliance.

Microsoft has a longstanding commitment to privacy. More than a decade ago, it was one of the first companies to appoint a chief privacy officer. Microsoft currently employs more than 40 people who focus on privacy full time, and hundreds of others across the company and around the world support privacy as part of their jobs. The company's commitment to privacy begins with the Microsoft Privacy Principles, which address accountability, notice, collection, choice and consent, use and retention, disclosure of onward transfer, quality assurance, access, enhanced security, and monitoring and enforcement.

Microsoft Approach

Microsoft implements its commitment to privacy in many ways, including the following:

EMAIL AND FILE PRIVACY Microsoft does not scan the contents of Office 365 or Outlook.com customers' email or OneDrive documents for the purpose of serving ads.

TRUST CENTERS The Windows Office 365 Trust Center, the Windows Azure Trust Center, Windows Intune Trust Center, and the Dynamics CRM Online Trust Center describe how Microsoft cloud services help protect information privacy and security.

DO NOT TRACK People are worried about online tracking and want to protect their privacy, which is why Do Not Track (DNT) is enabled in Internet Explorer 11. Customers can turn DNT off at any time.

WINDOWS 8.1 The Windows 8.1 operating system was built with privacy in mind. It provides customers with the broad range of controls they need to make appropriate privacy choices.

KINECT AND XBOX ONE Microsoft created Kinect and Xbox One from the ground up with built-in privacy controls and safeguards that put customers in charge of their entertainment experiences and allow them to customize how their personal information or data is, or is not, shared.

Policy Considerations

Policymakers can help further Privacy by Design efforts to address privacy and data security throughout the industry by promoting several important principles:

- **ENCOURAGE INDUSTRY-WIDE ADOPTION OF PRIVACY BY DESIGN** Encourage companies to embrace these concepts by adopting guidelines and processes to build privacy into products and services through design, development, and deployment.

- **ENSURE INNOVATIVE, TECHNOLOGY-NEUTRAL PROCESSES** Privacy by Design principles are fundamental and can be supplemented by consumer education, self-regulation, and carefully crafted legislation. Such legislation should provide incentives to adopt Privacy by Design processes that are technology-neutral and do not stifle product development and innovation.

- **DEVELOP GLOBALLY INTEROPERABLE BASELINE PRIVACY LEGISLATION AND STANDARDS** Privacy initiatives should facilitate the free flow of information, build trust, and encourage innovation. Because data flow is global, companies should strive to create greater interoperability of privacy regulations, policies, and standards on a worldwide basis.

Privacy in the Cloud

Key Points

- The advances and increased adoption of cloud computing raise important policy considerations, including shared data storage, geographic location of data, transparency, access, and security.
- Microsoft has been providing cloud services for a number of years; it has consistently worked to understand customers' concerns and requirements to develop solutions that include robust privacy and security features.
- Microsoft prioritizes the privacy, security, and compliance needs of its customers, and its enterprise cloud services— including Office 365, Microsoft Dynamics CRM Online, Windows Intune, and Windows Azure— incorporate industry-leading privacy protection, security safeguards, and regulatory compliance features.

For organizations throughout the world—including governments, nonprofits, and businesses— cloud computing has become a key part of their ongoing information technology (IT) strategy. Cloud services give organizations of all sizes access to virtually unlimited data storage while freeing them from the need to purchase, maintain, and update their own networks and computer systems. However, as organizations continue to take advantage of the benefits of cloud services, they must consider two main things: how to secure their data in the cloud and how to protect their private information.

The following are some of the specific concerns cloud service providers must consider:

SHARED DATA STORAGE

When the data from many customers is stored at a shared physical location, cloud providers must take appropriate steps to segregate that data in order to protect it from inappropriate use or loss. Additional safeguards include providing strong levels of encryption and proper controls for administrative access.

TRANSPARENCY AND ACCESS

Customers want to know where their data is stored, who has access to it, how it is used and shared, and what safeguards are protecting it. Cloud providers can address these concerns—and build trust, too—by providing contractual commitments, implementing transparent policies, and communicating them clearly to customers and regulators.

GEOGRAPHIC LOCATION OF DATA

As cloud computing evolves, traditional geographical limits on data storage and movement also shift. For example, data created in France using software hosted in Ireland could be stored in the Netherlands and accessed from the United States. Consequently, regulators and cloud computing customers want clearly defined policies and disclosures regarding the physical location of their data.

SECURITY

Customers rely upon their cloud service providers not only to store their data securely but also to keep it safe from loss, theft, or misuse.

Key Points

- Conflicting legal obligations and competing claims of governmental jurisdiction over data usage continue to limit cloud computing services and their adoption. Divergent rules on privacy, data retention, and other issues cause ambiguity and create significant legal challenges.

Microsoft Approach

Microsoft has been providing cloud services for a number of years and has consistently worked to understand customers' concerns and requirements to develop solutions that include robust privacy and security features. Microsoft prioritizes the privacy, security, and compliance needs of its customers and provides enterprise cloud services, including Office 365, Microsoft Dynamics CRM Online, Windows Intune, and Windows Azure. These services incorporate industry-leading privacy protection, security safeguards, and regulatory compliance features.

Microsoft works closely with regulators and has incorporated their feedback into its approach, enabling customers to use cloud services with confidence. The Microsoft approach to cloud privacy encompasses the following priorities.

MAINTAIN A HIGH LEVEL OF DATA SECURITY Office 365, Microsoft Dynamics CRM Online, Windows Azure, and Windows Intune meet or exceed ISO 27001, a security certification that sets out a series of physical, process, and management controls. Refer to each service's Trust Center for a link to their ISO certification.

USE CUSTOMER DATA ONLY TO PROVIDE THE SERVICE—NOT FOR ADVERTISING Microsoft believes that the data that enterprise customers host in cloud services belongs to those customers, and should not be used by a cloud provider for purposes other than to provide the customers' service. This concept is in the company's enterprise cloud service agreements and is explained on its Trust Center websites. Customer data is defined as "all the data, including all text, sound, software, or image files that a customer provides, or are provided on the customers' behalf, to Microsoft through use of the Online Services." Microsoft does not use customer data for purposes unrelated to providing the service, such as advertising. Additionally, each service has establisheda set of standards for storing and backing up data, and for securely deleting data upon request from the customer.

DESIGN SOLUTIONS TO MEET CUSTOMER COMPLIANCE NEEDS Microsoft invests in developing and improving compliance processes that enable it to meet a wide range of standards efficiently and effectively. For example, Microsoft convened experts from the academic, public, and private sector in a joint effort that resulted in crafting a Business Associate Agreement that was satisfactory for a variety of regulated entities, including universities and health systems. Likewise, Microsoft has collaborated with financial services customers and banking regulators to develop compliance solutions, which will satisfy certain access and oversight requirements that the customer alone could not satisfy.

SUPPORT THE EUROPEAN UNION MODEL CLAUSES EU data protection law prohibits transfer of EU customer personal data to countries outside the European Economic Area (EEA) unless there are adequate protections for that data. Microsoft provides a contractual commitment to the processes and protections in its online services in the form of a data processing agreement, including contractual terms approved by the EU, known as the Standard Contractual Clauses (Model Clauses). Microsoft customers can take comfort that, by signing EU Model Clauses with Microsoft to assure adequacy for EU data protection law, they have the strongest commitment available in the industry regarding data transferred from within the EU. The European Union's 28

data protection authorities, acting through their "Article 29 Working Party," have determined that the contractual privacy protections Microsoft offers to its enterprise cloud customers meet the current existing EU standards for international transfers of data. Microsoft is the first and only cloud provider to receive this type of approval. Europe's privacyregulators have said, in effect, that personal data stored in Microsoft's enterprise cloud is subject to Europe's rigorous privacy standards no matter where that data is located. This recognition applies to Microsoft's enterprise cloud services – in particular, Microsoft Azure, Office 365,Microsoft Dynamics CRM and Windows Intune. Microsoft also abides by the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S Department of Commerce regarding the collection, use, and retention of data from the EEA and Switzerland.

SEEK INDEPENDENT THIRD-PARTY AUDIT AND CERTIFICATION Microsoft obtains independent third-party audits, such as SSAE16 SOC1 and SOC2, and certifications, such as ISO 27001, so users can trust that its services are designed and operated with stringent safeguards.

MAINTAIN TRANSPARENCY Through its Trust Centers for Office 365, Microsoft Dynamics CRM Online, Windows Intune, and Windows Azure, Microsoft provides easy-to-understand information about where customer data is stored, who can access it, and the identity of any sub-contractors that may handle personal data. Customers can sign up to receive notifications about changes to geographic data flow information. Regarding requests for customer data from law enforcement or other governmental entities, Microsoft is firm in its commitment to protect customer data. It provides data only for lawful requests for specific sets of data. The company does not disclose customer data to a third party (including law enforcement, other government entity, or civil litigant) except as customers direct or as required by law. If a third party contacts Microsoft with a demand for customer data, the company tries to redirect the third party to request it directly from customer. If compelled to disclose customer data to a third party, Microsoft promptly notifies the customer and provides a copy of the demand, unless legally prohibited from doing so.

Policy Considerations

Policymakers can help boost consumer confidence and address concerns over data security and privacy in cloud computing by focusing on several priorities:

- **CREATE INTEROPERABLE DATA SECURITY AND PRIVACY LAWS ACROSS JURISDICTIONS** Conflicting legal obligations and competing claims of governmental jurisdiction over the use of data continue to limit cloud computing services and their adoption. Divergent rules on privacy, data retention, and other issues cause ambiguity and create significant legal challenges.

- **SUPPORT TECHNOLOGICAL INNOVATION AND INDUSTRY COLLABORATION** As governments develop policies that address the privacy and security concerns associated with cloud computing, they should continue to support technological innovation and its adoption. Working together, government and industry can establish appropriate privacy principles that protect data in the cloud.

Resources

GENERAL

Overview of Microsoft privacy policies and initiatives: **www.microsoft.com/privacy**

Microsoft Privacy Practices: **www.microsoft.com/privacy/principles.aspx**

Privacy Guidelines for Developing Software Products and Services (PDF, 1.16 MB):

aka.ms/privacy-guidelines

Privacy settings for Microsoft technologies: **www.microsoft.com/yourprivacy**

Microsoft Trustworthy Computing: **www.microsoft.com/twc**

FUTURE PRIVACY MODELS

Perspectives on evolving privacy models:

www.microsoft.com/en-us/twc/privacy/models.aspx

Microsoft Perspectives on Evolving Privacy Models (PDF, 126 KB):

www.download.microsoft.com/download/1/5/4/
154763A0-80F8-41C8-BE52-80E284A0FBA9/Evolving-Privacy-Models.pdf

MICROSOFT PRIVACY STATEMENTS

Microsoft Privacy Statement: **aka.ms/privacy-statement**

MICROSOFT CLOUD RESOURCES

Cloud Privacy: **www.microsoft.com/en-us/twc/privacy/cloud-privacy.aspx**

TRUST CENTERS

Microsoft Dynamics CRM Trust Center:

www.microsoft.com/en-us/dynamics/crm-trust-center.aspx

Office 365 Trust Center: **www.trust.office365.com**

Windows Azure Trust Center: **www.windowsazure.com/en-us/support/trust-center/**

Windows Intune Trust Center: **www.microsoft.com/en-us/WindowsIntuneTrust**

PRIVACY ACCOUNTABILITY

The Role and Importance of Organizational Accountability in Managing and Protecting Users' Data: **aka.ms/accountability-privacy**

Information Policy Centre - Accountability-related papers: **aka.ms/accountability-papers**

PRIVACY BY DESIGN AT MICROSOFT

Privacy by Design: **www.microsoft.com/privacy/bydesign.aspx**

PRIVACY IN THE CLOUD

Cloud Privacy at Microsoft: **www.microsoft.com/privacy/cloudcomputing.aspx**

Privacy in Microsoft advertising: **choice.microsoft.com**

Protecting Data and Privacy in the Cloud (PDF, 372 KB):

go.microsoft.com/?linkid=9694913

Law Enforcement Requests:

www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

Brad Smith Blog Post - Responding to government legal demands for customer data:

blogs.technet.com/b/microsoft_on_the_issues/archive/2013/07/16/responding-to-government-legal-demands-for-customer-data.aspx

GLOBAL PARTNERSHIPS AND INITIATIVES

Children's Online Privacy Protection Act:

www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

European Union Data Protection Directive:

ec.europa.eu/justice/data-protection/index_en.htm

Asia-Pacific Economic Cooperation Privacy Framework:

publications.apec.org/publication-detail.php?pub_id=390

Organization for Economic Co-operation and Development (OECD): **www.oecd.org/**

US – European Union Safe Harbor Framework:

www.export.gov/safeharbor/eu/eg_main_018365.asp

US – Switzerland Safe Harbor Framework: **www.export.gov/safeharbor/swiss/index.asp**

Microsoft

Online Safety

Building Global Trust Online, 4th Edition

Microsoft Perspectives for Policymakers

Online Safety at Microsoft: Building a Safer Digital World

Microsoft supports digital citizenship—safer, responsible, and more appropriate use of technology and devices.

What is online safety?

Online safety is the practice of maximizing desirable digital experiences and minimizing those tied to illegal, inappropriate, or illegitimate content, contact, conduct, or commerce – "The 4 Cs."

CONTENT

Users can be exposed to inaccurate, inappropriate, or objectionable content online.

CONTACT

Interactions online can lead to unwanted contact.

CONDUCT

How we act online affects our own reputation as well as others.

COMMERCE

Criminals attempt to steal sensitive personal information and money by breaking into business databases and personal accounts or through scam solicitations.

The Microsoft approach to online safety

Microsoft defines the discipline of online safety in terms of risk management. To help people minimize their risk online, Microsoft:

DEVELOPS TECHNOLOGY TOOLS

Microsoft offers a range of technologies for online safety.

- **MICROSOFT SECURITY ESSENTIALS**
- **INPRIVATE BROWSING**
- **SMARTSCREEN FILTER**
- **BING SAFESEARCH**
- **MICROSOFT FAMILY SAFETY TOOLS**
- **REPORT ABUSE MECHANISMS**

PROVIDES EDUCATION AND GUIDANCE

Microsoft puts its passion for online safety into practice by:

Offering guidance on how people can better secure their devices and help protect their information and families online through the Microsoft Safety & Security Center.

Conducting research, like the Microsoft Computing Safety Index, to gauge online safety behaviors and improve digital lifestyles.

ESTABLISHES PARTNERSHIPS

Everyone plays a role in helping to create a safer and better Internet.

PARENTS AND CAREGIVERS

EDUCATORS

TECHNOLOGY INDUSTRY

LAW ENFORCEMENT AND GOVERNMENT

NONGOVERNMENTAL ORGANIZATIONS

Read on to learn more about online safety at Microsoft

Online Safety

Key Points

- The Internet enriches lives in many ways, but it also presents risks to privacy, safety, personal and professional reputations, and commerce due in part to the online presence of cybercriminals and malicious software.
- Microsoft defines the discipline of online safety in terms of risk management. To help people minimize their risk online and to create safer, more trusted computing experiences, Microsoft develops technology tools; provides education and guidance; and partners with government, industry, law enforcement, and nonprofit organizations.
- Online safety is a shared responsibility, and government and industry must work together to support it.

The Internet has revolutionized the way we work, learn, communicate, and play. However, it has also created new risks and potential for harm. These include infection of devices by malicious software, such as viruses; victimization by online scammers selling counterfeit goods or pushing fraudulent investment schemes; loss of privacy; and identity theft by criminals.

Many people are concerned about these risks, but they often fall short in taking the steps necessary to protect themselves. Since 2011, the Trustworthy Computing group at Microsoft has sponsored the Microsoft Computing Safety Index (MCSI), an annual study that measures the actions that consumers take to help keep themselves and their families safe online. The 2013 MCSI sampled 10,500 adults in 20 countries and regions worldwide. Results showed that although users are cautious (for example, conducting transactions on reputable websites and using strong passwords), they often miss taking active steps to keep themselves safer, such as locking mobile phones or adjusting privacy settings on social sites.

Addressing the challenges of online safety requires collaboration between the technology industry and government. Technology companies must commit to protecting sensitive data and personal information as well as facilitating business practices that promote trust. Governments can support industry self-regulation and legislative frameworks that foster an environment of technological innovation.

Microsoft Approach

Grounded in its Trustworthy Computing initiative, Microsoft has a longstanding commitment to online safety, which the company's Chief Online Safety Officer oversees. The Chief Online Safety Officer is responsible for all aspects of Microsoft online safety strategy, which includes creating and implementing internal policy, influencing the development of safety features and functionality in Microsoft products and services, and engaging with an array of external audiences. Microsoft defines the discipline of online safety in terms of risk management. The company views its role as helping people maximize desirable online experiences while minimizing the risks by:

DEVELOPING TECHNOLOGY TOOLS

- Microsoft Security Essentials, a free antimalware program, is available for download.
- Microsoft account holders can specify who may view their profiles, who can contact them, and who can post or view the content they share. Internet Explorer also helps manage people's privacy with InPrivate browsing and the SmartScreen Filter that helps warn users about phishing sites.
- Microsoft offers family safety tools to help protect children online in all editions of Windows 7 and 8, on Windows Phone, and in Xbox products and services. Bing provides the SafeSearch feature, which can help keep adult content out of kids' search results.

PROVIDING EDUCATION AND GUIDANCE

- The Microsoft Safety & Security Center offers tips and advice on how people can better secure their devices, protect their reputations and families online, and evade online scams.

- The Microsoft Safer Online team raises public awareness about online safety habits and practices through its participation in such events as Safer Internet Day and National Cybersecurity Awareness Month, as well as presentations at the Internet Governance Forum

PARTNERING WITH OTHERS

- Microsoft works with nongovernmental organizations, law enforcement, and other technology companies on online safety issues. The company collaborates with organizations like the Family Online Safety Institute (FOSI) and the National Cyber Security Alliance (NCSA).

- Microsoft developed and shared PhotoDNA, a technology that helps nongovernmental organizations, law enforcement, and other technology companies find and remove from the Internet some of the worst images of child sexual abuse.

- The company offers technical training to law enforcement agencies and develops new tools to help them combat cybercrime. Microsoft also works with law enforcement to stop cybercriminals through legal action, including steps to take down botnets and shut down the purveyors of fake security software.

Policy Considerations

SUPPORT INNOVATION AND SELF-REGULATION As governments address the risks associated with emerging technologies and online services, it is important that they support industry self-regulation and legislative frameworks that foster an environment of technological innovation.

ENCOURAGE PUBLIC-PRIVATE PARTNERSHIPS Government and industry can work together to establish safety principles and help service providers fulfill their safety promises. Examples include ISP codes of practice in Australia (and other countries) to help secure a fair and open Internet,[1] recommendations from the EU CEO Coalition[2] to make the Internet a safer place for children, and the UK Search Engine agreement to block illegal search terms and images of child sexual abuse.[3]

SUPPORT RESEARCH THROUGH COMMISSIONS AND FUNDING Research plays a critical role in identifying factors that increase online risk and in dispelling myths that can lead to misplaced efforts to address them. Government commissions and funding to advance Internet safety are essential to support both academic and industry research.

PROMOTE ONLINE SAFETY EFFORTS IN EDUCATION Online safety curricula should become an integral part of schools' efforts to achieve technological literacy for their students, and should weave into the standard curricula modules that focus on digital literacy and civility.

---

1 *Internet Industry Code of Practice Version 6:* iia.net.au/codes-of-practice/internet-industry-code-practice-version-6.html
2 *Self-Regulation for a Better Internet for Kids:* aka.ms/EC-SaferInternet
3 www.gov.uk/government/news/internet-safety-summit-at-downing-street-communique

Digital Citizenship

Key Points

- The Internet presents great opportunities, but it is not without real risk of experiencing inappropriate content, contact, conduct, or commerce. The risks can be mitigated by teaching digital literacy and civility—elements that are central to good digital citizenship.
- Microsoft created the Digital Citizenship in Action Toolkit expressly to teach young people and adults how to become good digital citizens, and the company promotes digital literacy programs in 134 countries.
- Education policymakers should broaden online safety efforts and adopt a set of national goals for online safety, including minimum standards for digital literacy curricula.

New information technologies have profoundly changed the world—the immense resources of the Internet and the accompanying array of Internet-enabled devices and services give everyone tremendous opportunities to work, learn, communicate, and play. While largely positive, the Internet has also created new potentials for harm. These include infection by malicious software, such as viruses, worms, and spyware; victimization by online scammers selling counterfeit goods or pushing fraudulent investment schemes; loss of privacy and damage to online reputation; and identity theft by criminals.

Governments, the technology industry, and public sector organizations have addressed this risk to online safety through technology tools, policies, law enforcement activities, and education. These approaches play important roles, but to be successful, strategies (educational approaches in particular) must take into account the social norms and behaviors that everyone, including young people, must understand to become responsible digital citizens.

The concepts of digital citizenship—the safer, more responsible, and appropriate use of technology and devices—underpin such an approach. In becoming good digital citizens, people develop a sense of ownership and personal responsibility that will help them make ethical decisions in the online world, and in so doing build a safer, more trusted Internet. Digital citizenship is grounded in two primary elements: digital literacy and civility.

DIGITAL LITERACY Those who are literate in the online world are better prepared to avoid risky situations, make better-informed decisions, and better understand how to protect their privacy. They have learned such basic online safety habits as how to protect their accounts and reputation, the importance of strong and secret passwords, and how to update their computers and devices to defend against malware and scams. Digital literacy also requires the critical thinking skills needed to evaluate online information and situations and to problem-solve.

DIGITAL CIVILITY Digital literacy provides a solid foundation for digital citizenship, but Internet users must also demonstrate respect for others—behaving with civility and being protective of everyone's rights (their own included). People must learn and apply the skills to behave ethically and within online social norms. These skills include being judicious about what they say and do online; protecting others' privacy by not sharing personal details of friends and family without their permission; and respecting the intellectual property of others—for example, downloading only legal copies of copyrighted material.

Microsoft Approach

MATERIALS TO TEACH DIGITAL CITIZENSHIP The Digital Citizenship in Action Toolkit was created expressly to teach people how to become good digital citizens. Fact sheets, tip cards, videos, and other materials give information about safer social networking, inappropriate behavior (like online bullying), using mobile devices more safely, responsible online gaming, and protecting oneself from online fraud and identity theft.

WORLDWIDE SAFETY EDUCATION PROGRAMS Microsoft promotes digital literacy programs in 134 countries with a particular focus on broadening the reach beyond those who speak English and other commonly used languages. Programs include Partners in Learning and YouthSpark.

SUPPORT FOR ONLINE SAFETY CURRICULA IN SCHOOLS Microsoft believes that digital citizenship is an important component of any school curriculum; it supports the integration of digital citizenship concepts in technology instruction for students, with key topics woven into existing curricula.

Policy Considerations

Policymakers in government and industry can help companies work more securely on the Internet and protect company data and financial assets against cybercrime by adhering to the following principles:

- **EMPHASIZE DIGITAL CITIZENSHIP EDUCATION** Education policymakers should broaden online safety efforts to include an emphasis on digital citizenship through digital media literacy and education programs. They should also adopt a set of national goals for online safety, including minimum standards for digital literacy curricula.

- **SUPPORT FUNDING OF DIGITAL CITIZENSHIP PROGRAMS** Governments should ensure that all digital literacy and online safety programs are funded through competitive grants open to qualified applicants, with periodic review and assessment built in so that the results from the best programs can be replicated in other communities.

- **PROVIDE LEGISLATION SUPPORTING DIGITAL SAFETY CURRICULA** Some jurisdictions require that online safety education be an integral part of school system efforts to achieve digital literacy for their students. Legislation requiring schools to implement online safety education should be broad enough to account for local variations in curricula. One example is a US law mandating that Internet safety be included in the curricula of any school that receives E-Rate funding[4] from the Federal Communications Commission (FCC), which gives schools and libraries discounts for telecommunications and Internet access.

- **PROMOTE INDUSTRY SELF-REGULATION AND INNOVATION** As governments address the risks associated with emerging technologies and online services, it is important that they support industry self-regulation and legislative frameworks that encourage technological innovation.

---

4 *Laws Require Internet Safety Education in Schools that Receive E-Rate Funds:* aka.ms/E-Rate_online_safety_educ

Child Online Safety

Key Points

- Although the Internet enables many enriching experiences for children, there are also risks, including potential exposure to inappropriate content, contact with bullies, and loss of privacy.
- The Microsoft approach to children's online safety includes creating innovative technology tools; providing education and guidance; establishing robust internal policies and practices for moderating content and addressing online abuses; and partnering with nongovernmental organizations, industry, law enforcement, and others.
- The safety of children online is a community challenge and government, industry, and others should work together to establish and implement safety principles. As governments address risks associated with emerging technologies and online services, it is important that they continue to encourage innovation and technology adoption.

Although the Internet offers a wealth of positive experiences for children, parents face challenges when monitoring the content their children encounter online, the people they meet there, and what they share.

INAPPROPRIATE CONTENT

Young people are curious and may stumble upon inappropriate material (including hateful or sexual content) by clicking a link in email, on a social network, or while searching for something else on the web.

INAPPROPRIATE CONDUCT

Young people—and adults, too—may use the Internet to harass or exploit others. Kids may sometimes broadcast hurtful bullying comments or embarrassing images. A particular concern with mobile devices is sexting—the transmission of sexually explicit photographs and videos taken with a device's camera.

INAPPROPRIATE CONTACT

Adults—and young people, too—use the Internet to find and approach vulnerable youth. Frequently, their goal is to develop what youth believe to be meaningful online relationships, a process referred to as *grooming*.

INAPPROPRIATE COMMERCE

Children can easily fall victim to phishing or other scams. They can be enticed to click a flashy ad, open an appealing "free" game, or download a ringtone. These can install viruses, spyware, or other malicious software.

Microsoft Approach

The Microsoft approach to combating child safety issues on the Internet includes developing technology, providing education and guidance, establishing internal policies, and partnering with others.

CREATING TECHNOLOGY TOOLS Microsoft builds safety features into a wide range of its products and services to help parents minimize online risks to their children.

In all editions of the Windows 7 and Windows 8 operating systems, parents can use the Family Safety feature to create a separate account, with specific activity limits, for each family member.

The Xbox platform is equipped with parental controls to help create a safer environment for all gamers. For example, on Xbox One, parents can use Family and Online Safety controls to set a maximum age, which maps to ratings systems like Entertainment Software Rating Board (ESRB) and Pan European Game Information (PEGI).

Windows Phone offers two ways to manage young people's access to games and apps. Young people under age 18 who have their own Windows Phone sign in with a child's account. Parents set up My Family, add the young person, and then manage what kids can download from the Windows Phone Store. For younger ones, parents can use Kid's Corner to create a space on their phone where children can play games, use apps, and watch videos that parents have selected.

Bing SafeSearch can help keep adult content in text, images, and videos out of children's search results.

PROVIDING EDUCATION AND GUIDANCE The Microsoft Safety & Security Center provides age-based advice for Internet use, and guidance on such issues as online bullying, safer social networking, mobile device safety, responsible online gaming, and how to avoid, block, and report inappropriate behavior.

ESTABLISHING INTERNAL POLICIES AND PRACTICES Microsoft promotes online safety through robust company-wide policies, standards, and procedures for its web products and services. It enforces policies inherent in its code of conduct for users of its online services, and it moderates content and interactions to address illegal activity, inappropriate material, and other abusive content or contact.

PARTNERING WITH OTHERS To help promote online safety for children and young people, Microsoft:

Collaborates with industries and organizations like the Family Online Safety Institute, which sponsored A Platform for Good to start a dialogue about what it means to participate responsibly in a digital world.

Developed and shared PhotoDNA, an image-matching technology that helps nongovernmental organizations, law enforcement, and other technology companies such as Facebook and NetClean find and remove some of the worst images of child sexual abuse from the Internet.

Policy Considerations

Governments and other policymakers can help promote recent efforts in child online safety by focusing on these priorities:

- **STRENGTHEN AND ENFORCE EXISTING CHILD PROTECTION LAWS** Governments must strengthen and enforce laws against the possession and distribution of child sexual abuse images. Microsoft works with the International Center for Missing & Exploited Children (ICMEC), INTERPOL, and other organizations to support government efforts.

- **ENCOURAGE PUBLIC-PRIVATE COLLABORATION** Government and industry must collaborate to establish safety principles and offer a more secure online environment for youth. Examples of this collaboration include recommendations from the EU CEO Coalition[5] to make the Internet a safer place for children, the UK search engine agreement to block images of child abuse,[6] and the digital citizenship principles published by the Australian Communications and Media Authority (ACMA).[7] As governments address risks associated with emerging technologies, they must avoid stifling innovation and technology adoption.

- **PROMOTE COMPREHENSIVE ONLINE SAFETY EDUCATION IN SCHOOLS** Programs should include modules that weave digital literacy (including how to avoid online dangers and protect devices) and digital civility into the standard curricula. Legislation requiring schools to implement online safety education should be broad enough to accommodate local variations in curricula.

- **SUPPORT INTERNET SAFETY RESEARCH** Research is particularly important for identifying factors that increase online risk and for dispelling myths that can lead to misplaced efforts to advance Internet safety. Government funding for both academic and industry research in these areas is essential.

5 *Self-Regulation for a Better Internet for Kids:* aka.ms/EC-SaferInternet
6 www.gov.uk/government/news/internet-safety-summit-at-downing-street-communique
7 www.cybersmart.gov.au/cybersmart-citizens.aspx

Online Safety Education

Key Points

- The Internet is an extraordinary tool for enabling young people to learn about and explore the world around them, but it may also expose them to certain risks, such as inappropriate content, contact, conduct, or commerce. Comprehensive online safety education is a crucial part of teaching young people to address these risks and build the skills of good digital citizenship.

- Microsoft offers age-based guidance to help teach young people about online safety, promotes digital literacy programs in 134 countries, and encourages its employees to get involved in online safety education.

- Microsoft supports comprehensive online safety education in schools, with key topics woven into the existing curriculum. Legislation requiring schools to implement online safety education should be broad enough to account for local variations in curricula.

The immense resources of the Internet and the accompanying array of Internet-enabled devices give young people tremendous opportunities to learn, share, and communicate. Online, however, youth may be exposed to certain risks. These may include potential exposure to inappropriate content (including sexually explicit or hateful websites), contact (from predators), conduct (such as bullying or inappropriate sharing), or commerce (like identity theft or pirated music and games).

Comprehensive and age-appropriate online safety education plays a vital role in helping young people learn about those risks and how to avoid them. They'll learn this best in the context of developing positive online behaviors, such as respect for intellectual property and adherence to basic codes of acceptable conduct. This is often referred to as digital citizenship, the norms of behavior in online society. Learning these norms prepares young people to be good digital citizens in technology-rich societies. It helps them develop a sense of ownership and personal responsibility that, in turn, will help them make appropriate, ethical decisions in the online world.

Ideally, given the vast array of diverse subject material that educators much teach every day, the principles of digital citizenship should be woven into the existing curricula.

DIGITAL LITERACY

Young people should learn basic online safety habits: how to protect their accounts and reputation; the importance of strong and secret passwords; and how to update their computers and devices to defend against viruses, spam, and phishing scams. Digital literacy involves more than just technical competency—it requires critical thinking skills to evaluate different sources of information and situations, to solve problems as they arise, and to know when to report problems to the appropriate adults.

DIGITAL CIVILITY

Young people should learn the risks of bullying, plagiarism, and piracy, and learn the skills to behave ethically and operate within online social norms. These skills include standing up for friends, not sharing personal details of friends and family without their permission, downloading only legal copies of copyrighted material, and using social networks that are right for their age.

Microsoft Approach

The company makes contributions to online safety education that include the following:

The Microsoft Safety & Security Center provides age-based guidance—both online and in face-to-face training sessions and similar events—to help young people become good digital citizens with information about online bullying and inappropriate online behavior, safer social networking, safer use of mobile devices, and responsible online gaming.

Microsoft employees in 26 of its European subsidiaries reach more than 90,000 teachers, parents, and students. For example, in the United Kingdom and Australia, Microsoft employees developed a program called ThinkUKnow with local law enforcement officials to deliver online safety education and resources.

Microsoft promotes online safety and digital literacy programs in 134 countries, with a particular focus on broadening the reach beyond those who speak English and other commonly used languages. Activities include Partners in Learning, YouthSpark, the Unlimited Potential, and Community Technology Access programs.

Policy Considerations

Governments and other policymakers can help promote recent efforts in online safety education by focusing on these priorities:

- **SUPPORT ONLINE SAFETY EDUCATION EFFORTS IN PUBLIC SCHOOLS** A number of jurisdictions require that online safety education be an integral part of school system efforts to achieve digital literacy for their students, which is a trend that must continue and grow. For example, one US law mandates that anti-bullying measures be taught in any school that receives E-Rate funding from the Federal Communications Commission (FCC), which gives schools and libraries discounts for telecommunications and Internet access.[8]

- **SUPPORT TECHNOLOGY TRAINING FOR TEACHERS** Just as students need education about safer Internet use, teachers also need training to keep up with ever-changing technology. Teacher training for effective use of technology in the classroom must include an understanding of current Internet risks, recognition of when students may be subject to online dangers, and guidance for helping students conduct themselves with civility on the web.

- **BALANCE ONLINE RESTRICTIONS WITH SAFETY EDUCATION** Restricting children's Internet access may be appropriate in some areas, such as where age limits currently exist in the physical world—like gambling and pornography. But safety experts agree that restricting access is not enough and that education plays a vital role in the safety of young people online.

8 *Laws Require Internet Safety Education in Schools that Receive E-Rate Funds:* www.safeschools.info/bullying-prevention/bullying-prevention-news/362-laws-require-internet-safety-education-in-schools-that-receive-e-rate-funds

Family Safety Settings

Key Points

- Family safety settings help parents monitor their children's Internet use. Although they are not a substitute for parental involvement, family safety technologies can help reduce the risk of exposure of young people to inappropriate content, contact, conduct, and commerce.
- Microsoft has long provided the tools (including in Windows, Xbox, and Windows Phone) that parents need to help them put their decisions into practice in a way that supports their values and the maturity of their children.
- Decisions about what children can view online are best left to parents and caregivers, so Microsoft does not support efforts to require the use of parental controls or filtering software. Instead, governments must work with industry and nongovernmental organizations to help promote and publicize online safety technology.

Although the Internet offers many enriching opportunities for young people, there are also concerns about the content they encounter, the people they meet there, and what they share. One way to help protect youth is through technologies that parents and caregivers can use to monitor what children and teens are seeing, hearing, and doing online.

These family safety (or parental control) technologies—including content filters, contact management tools, and limits on the download and use of music, apps, and other files—have been used on personal computers since the early 1990s. Now, as mobile phones, tablets, and other devices have become Internet-enabled, technology companies have added family safety settings to them as well.

Family safety settings are widely used in many countries. In 2011, a survey in the United States by the Family Online Safety Institute (FOSI)[9] found that 54 percent of parents used them. Microsoft research in 2012 of 1,000 parents in Brazil, China, France, India, and the United States found that they were split between monitoring their children's online activity (43 percent) and limiting access (45 percent).

Despite their popularity and obvious utility, parental controls have generated controversy. Some have advocated that governments should mandate their use by minors; others have pushed for mandatory use by everyone, a position that human rights advocates and others strongly oppose; still others raised concerns about the misuse of such technology for spying by overzealous parents.

Microsoft Approach

Microsoft believes that the company's role in providing family safety tools is to help parents put their decisions into practice in a way that supports their values and the maturity of their children.

WINDOWS 7 AND WINDOWS 8 offer parents Family Safety, which they can use to create a separate account for each family member. Parents can then monitor where their children go and what they do online. For more control, parents can set daily time limits and block websites they specify.

WINDOWS PHONE offers two ways to manage the access of young people to games and apps:

- Young people under age 18 who have their own Windows Phone sign in with a child's account. They won't be able to download anything until parents set up My Family and add the young person. Once that's done, parents can manage the apps and games that their children can download from the Windows Phone Store.

9 Who Needs Parental Controls? A Survey of Awareness, Attitudes, and Use of Online Parental Controls: **www.fosi.org/research/900-who-needs-parental-controls.html**

- For younger ones, parents can use Kid's Corner to create a space on their phone where children can play games, use apps, and watch videos that parents have selected. While in Kid's Corner, the child can't purchase apps and won't be able to access functions that might not be age appropriate, such as web browsing or text messaging.

XBOX Microsoft was the first to produce a gaming console that introduced ratings-based parental controls.

- Xbox 360 Family Settings enable parents to set and enforce content ratings for games, movies, and television shows; they can also set limits on console play time using the family timer.

- On Xbox One, parents use Family and Online Safety controls to set a maximum age, which maps to ratings systems like Entertainment Software Rating Board (ESRB) and Pan European Game Information (PEGI). Parents can then decide whether they want Xbox One to always block content that exceeds this rating or make that decision on a case-by-case basis.

- With Online Safety Settings for Xbox Live, parents can create individual profiles that are appropriate for each child's age and maturity. Parents can specify what activities children can participate in (such as multiplayer gaming, video chat, text messaging, or voice messaging), who they can communicate with, and who can see the child's profile or friends list.

Policy Considerations

Policymakers can help make technology and the Internet safer for families by promoting the following principles:

SUPPORT SELF-REGULATION INSTEAD OF MANDATORY COMPLIANCE Decisions about what children can view online are best left to parents and caregivers, so Microsoft does not support efforts to require the use of parental controls or filtering software. Instead, government must work with industry and nongovernmental organizations such as GetNetWise to help promote and publicize online safety technology.

ADDRESS RISKS IN EMERGING TECHNOLOGY WITHOUT STIFLING INNOVATION To better protect young people online, industry must regulate itself and government must develop thoughtful legislative frameworks for addressing risk in emerging technology areas. As governments do this, it is essential that they allow for innovation in the process.

PROMOTE SAFETY THROUGH COLLABORATION Government and industry must work together to establish safety principles that will help create a more secure online environment. Examples of this collaboration include the ISP codes of practice in Australia (and other countries) to help secure a fair and open Internet, recommendations from the EU CEO Coalition to make the Internet a better place for kids, and the UK Search Engine agreement to block illegal search terms, as well as images and video of child sexual abuse.

ENCOURAGE INTERNET INDUSTRY COOPERATION Policymakers should support legislation that releases access providers from liability for obscene material or abusive behavior if they have made a good-faith effort to screen their services or provided screening devices for parents. Examples include Section 230 of the US Communications Decency Act and the European Union Directive 2000/31/EC.

Microsoft Computing Safety Index

Key Points

- Microsoft uses the Microsoft Computing Safety Index (MCSI) annually to identify and rate the online security- and safety-related behaviors of people around the world. Microsoft's research, combined with the resulting Index, will help lead to safer technologies and programs for better educating web users.
- The Microsoft approach to online safety includes developing technology tools; providing education and guidance; and collaborating with industry, law enforcement, and nonprofit organizations.
- Policymakers can advance the impact of online safety by supporting and funding research to promote public awareness of online safety issues, as well as by encouraging innovation and self-regulation.

As more people connect online, the need for safety, security and privacy grows. Consumers are increasingly concerned about security breaches, fraud, and the collection and use of personal information. Microsoft believes that a better understanding of how people respond to and defend against these threats can help lead to safer technologies and better programs for educating web users.

Since 2011, Microsoft has fielded the Computing Safety Index, a survey that measures the steps people report taking to protect their computers, mobile phones, and information online. The survey organizes 24 protective steps into three categories. The more steps respondents report taking, the higher their Index score, with 100 being the highest rating.

- **BEHAVIORAL:** seven protective behaviors, from using unique passwords for each account or website to educating oneself about the most current ways to protect one's online reputation and defend against identity theft
- **TECHNICAL:** twelve technology tools that include using privacy settings, limiting what others can see on social sites, and locking mobile devices with a PIN or password
- **FOUNDATIONAL:** five basic protections like leaving the computer's firewall turned on and running automatic software updates

In May 2013, researchers surveyed more than 10,000 people age 18 and older in 20 countries and regions around the world.[10] They found that the steps people take to protect themselves online haven't changed much since the first survey.

When respondents checked their settings, researchers found that people scored relatively well on those foundational protections that are built into devices and software by technology companies.

10 Australia, Belgium, Brazil, Canada, China, Egypt, France, Germany, India, Indonesia, Japan, Korea, Malaysia, Mexico, Russia, Singapore, Spain, Turkey, the United Kingdom, and the United States

However, by a large margin (60 percent), people see themselves as best able to protect their information rather than relying on technology companies, government, and others.

That doesn't seem to be the case.

- Only one in five (21 percent) of those surveyed took advantage of web browser filters that help protect against phishing.
- Just 31 percent educated themselves about the latest steps for protecting their online reputation or were selective about what they texted.
- Only slightly more than one-third said they limit the amount of personal information that appears online (36 percent) or educate themselves about the most current ways to protect against identity theft (37 percent).

THE RESULT?

15% *of respondents said they or someone they know had been victims of a phishing attack*

13% *experienced damage to professional reputation*

9% *said their identity had been compromised*

Microsoft Approach

The Microsoft approach to online safety includes developing technology tools, providing education and guidance, and engaging through policy with governments and nonprofit organizations.

DEVELOPING TECHNOLOGY TOOLS Microsoft offers free technology tools to reduce online risk, including Microsoft Security Essentials, a free antimalware program. Internet Explorer offers settings to help people manage their privacy online, including InPrivate browsing, as well as the SmartScreen Filter that helps warn users about potential phishing websites. In addition, Microsoft has built family safety features into many of its products, including all editions of Windows 7 and 8 with Microsoft Family Safety (which helps monitor and protect children online), Windows Phone, and Xbox products and services.

PROVIDING EDUCATION AND GUIDANCE For decades, Microsoft has invested in consumer awareness about the safer use of technology and the Internet.

- The Microsoft Safety & Security Center offers online safety guidance to consumers. This includes tips for safer social networking, use of mobile devices, and online gaming, as well as guidelines for avoiding, blocking, and reporting inappropriate behavior.

- Microsoft has commissioned many studies in addition to the MCSI. These included surveys of parents and non-parents about kids' access to devices and online services, mobile phone manners and safety habits, as well as surveys of consumer concerns about online privacy and their personal information online.

ENGAGING THROUGH POLICY WITH GOVERNMENTS AND NONPROFIT ORGANIZATIONS Microsoft efforts have centered on engaging through public policy with governments around the world, as well as with nongovernmental organizations such as the National Cyber Security Alliance and the Family Online Safety Institute, and on such online safety initiatives as National Cyber Security Awareness Month, Safer Internet Day, and STOP. THINK. CONNECT.

Policy Considerations

Governments and policymakers can aid in fighting online security risks and help encourage safer online behavior by focusing on the following:

SUPPORT RESEARCH THROUGH COMMISSIONS AND FUNDING Research (like the MCSI) plays a critical role in identifying factors that increase online risk and in dispelling myths that can lead to misplaced efforts to address them. It is essential that government commissions and funding support Internet safety research.

PROMOTE PUBLIC AWARENESS OF ONLINE SAFETY Governments and technology companies worldwide should invest in Internet safety by supporting programs aimed at increasing public awareness of Internet risks and guidance to help people avoid those risks.

ENCOURAGE INNOVATION AND SELF-REGULATION As governments address the risks associated with emerging technologies and online services, it is important that they support industry self-regulation and legislative frameworks that foster an environment of technological innovation, as well as promote cooperation between government and the technology industry.

Combating Child Exploitation Online

Key Points

- The Internet serves many beneficial and constructive purposes, but it has also created avenues for criminals to exploit young people through the distribution of child sex abuse images and the trafficking of children for sexual purposes.

- Microsoft aids in the advancement of technology, techniques, and processes to combat the use of the Internet to exploit children. These efforts include the development of technology (like Microsoft PhotoDNA) that can detect images of child exploitation, as well as partnerships with law enforcement agencies and nongovernmental organizations devoted to the cause.

- It is essential to enact and enforce laws against the possession, production, and distribution of child pornography worldwide, and to both build and fund the necessary infrastructure to ensure safe rescue, support, and recovery for victims of child sexual exploitation.

Every day, millions of people connect and share content on the Internet in beneficial and constructive ways. But the Internet has also created new avenues for criminals to exploit young people, such as through the distribution of child sex abuse images (also known as child abuse images), the trafficking of children for sexual purposes, and the grooming of children for sexual exploitation.

The production and distribution of child pornography represents a significant global law enforcement problem. Since 2002 (when its Child Victim Identification Program was created), the National Center for Missing & Exploited Children (NCMEC) has reviewed and analyzed more than 96 million images and videos of child sex abuse. These images are often found after pedophiles share and trade them amongst themselves and with others who reinforce their shared sexual interest in children.

As of 2011, most of the child pornography victims identified by NCMEC were prepubescent, with infants and toddlers the fastest-growing age category. Internet companies have an important role to play in helping fight this horrific trade by acting quickly to find, report, and eliminate these illegal images.

Another form of child exploitation is child predators' use of the Internet to find victims. These predators take advantage of the Internet's anonymity to build online relationships with young people or to communicate with those who traffic children for sex. As in the fight against images of child sex abuse, Internet companies have an important function in stopping predators and child sex traffickers. They can enforce codes of conduct, provide mechanisms for customers to report predators, and invest in innovation for improved detection.

Globally, law enforcement is doing admirable work to combat the online exploitation of children, but the scale of this problem requires broader cooperation from law enforcement, government, industry, nongovernmental organizations, and academia.

Microsoft Approach

COMBATING CYBERCRIME The Microsoft Digital Crimes Unit is an international legal and technical team working with partners to address technology-facilitated crime. With the opening of the Cybercrime Center in late 2013, Microsoft brought its cybercrime experts— attorneys, investigators, business professionals, and forensic analysts from around the world—together under one umbrella to help them better coordinate and collaborate to address cyberthreats.

COMBATING ILLEGAL IMAGES

- Microsoft applies filtering tools and employs highly trained experts using cutting-edge technology to help detect and classify images of child abuse that are shared on Microsoft services, such as Bing. The company reports these images to NCMEC, removes them, and bans the perpetrators from the services.

- In 2009, Microsoft Research collaborated with Dartmouth College and NCMEC to develop an advanced technology called PhotoDNA, which helps to refine and automate the search for child sex abuse images among the billions of photos on the Internet. NCMEC used the PhotoDNA license to work with online services such as Facebook to uncover images of child abuse. Since then, it has become the industry standard for detecting such images.

PARTNERING WITH OTHERS Microsoft partners with law enforcement and others around the world.

- In 2012, Microsoft worked with NetClean to make PhotoDNA image-matching technology available to law enforcement at no cost, in order to aid in investigations of the sexual exploitation of children.

- The company collaborates with the Thorn Technology Task Force (whose members also include Facebook, Twitter, and Google) to explore new ways technology can address the problem of child exploitation.

- In 2011, Microsoft issued a request for proposals for academic research into the role of technology in the sex trafficking of children. In 2012, Microsoft distributed $185,000 to six winning teams whose research results will be released as they are completed in 2014.

Policy Considerations

Policymakers can help address the challenges of combating child exploitation online by supporting the following efforts:

SUPPORT VICTIM RECOVERY SERVICES. Funding and infrastructure for effective victim recovery services is absolutely essential. Without this, any other interventions have the potential to do more harm than good.

ENACT LAWS THAT PROTECT VICTIMS OF CHILD EXPLOITATION It is vital that governments enact and enforce:

- Child exploitation laws that recognize and protect victims while holding traffickers accountable.

- Laws against the possession, production, and distribution of child sex abuse images worldwide. In 2012, the International Centre for Missing & Exploited Children (ICMEC) reported that 100 countries have "enacted new laws to protect children from child pornography." However, 53 countries have no laws at all, and 127 countries do not have laws that ICMEC considers sufficient.[11]

SUPPORT INDUSTRY-WIDE BEST PRACTICES AND GUIDANCE Internet companies must continue to work with governments and law enforcement to help address the problem of online predators by establishing industry best practices and guidance. More emphasis must be placed on enabling companies to voluntarily find and report images of child sex abuse. Policymakers can help change the focus of law enforcement to a model that measures their activities to stop crime and prevent abuse without penalizing the victim.

11 *ICMEC 2012 Highlights:* www.icmec.org/en_X1/icmec_publications/ICMEC_Highlights_2012.pdf

Combating Child Grooming Online

Key Points

- Grooming, the process by which predators manipulate children for sexual exploitation, is facilitated online when sexual predators use the Internet to make contact and develop relationships with children.
- The Microsoft approach to combating child predation includes creating innovative technology tools; providing education and guidance; establishing robust internal policies and practices for moderating content and addressing online abuses; and partnering with government, industry, law enforcement, and others.
- Microsoft strongly supports enacting and enforcing laws against the sexual exploitation of children, and cooperates with law enforcement to bring Internet pedophiles to justice.

Child grooming is a process of emotional manipulation by which pedophiles prepare children and youth for sexual exploitation. The grooming process typically involves an adult befriending a young person and then winning his or her trust by showering the youth with flattery, sympathy, gifts of money or modeling jobs, and other personal attention. The groomer then tries to sexualize the relationship, seeking to control the child and continue the abuse, which may include images of child sexual abuse or sex trafficking.

Pedophiles go where children go, and today that includes the Internet. Child grooming goes online when pedophiles use the Internet for the grooming process. Adults may begin the grooming process by visiting forums where youth interact, such as online games (which may use two-way voice and video technology) or chat rooms, or they may contact children through text messages. Pedophiles use the information that children reveal about themselves online to target vulnerable youngsters with low self-esteem, family or social issues, or lack of resources.

Sexual exploitation of children is a global problem. However, it is important to keep the online portion of the problem in perspective. According to the Crimes Against Children Research Center in the United States, the arrest of more than 600 online predators in 2006 constituted about one percent of all arrests for sex crimes committed against children and youth.

Internet companies have an important role to play in helping to stop predators. They can enforce codes of conduct, deploy monitors in forums used by children, and provide mechanisms for customers to report inappropriate conduct.

Microsoft Approach

The Microsoft approach to combating child grooming online includes developing technology, providing guidance, establishing internal policies, and partnering with others.

CREATING TECHNOLOGY TOOLS Microsoft builds safety features into a wide range of its products and services to help parents watch over their children online. For example, Windows 8 Family Safety offers tools to help parents monitor their children's online activities. Anyone—adult or young person—with a Microsoft account can specify who can view their profiles or contact them. In addition, Xbox Live has Online Safety Settings that enable parents to restrict who children can communicate with and who can see their profiles or friends lists.

PROVIDING EDUCATION AND GUIDANCE The Microsoft Safety & Security Center provides age-based guidance for Internet use, including tips on teaching children what's appropriate to view and share online; how to stay safer on mobile devices and in online games; and how to avoid, block, and report inappropriate behavior.

ESTABLISHING INTERNAL POLICIES AND PRACTICES To protect users on its online services, Microsoft enforces policies inherent in its code of conduct for users of its online services (such as Xbox Live), and moderates content and interactions to address illegal activity, inappropriate material, and other abusive content or contact.

PARTNERING WITH OTHERS Combating child predation requires a holistic approach in which technology providers, government leaders, law enforcement, and nongovernmental organizations all play vital roles.

- The Microsoft Digital Crimes Unit is an international legal and technical team working with partners to address technology-facilitated crime. With the opening of the Cybercrime Center in late 2013, Microsoft brought its cybercrime experts—attorneys, investigators, business professionals, and forensic analysts from around the world—together under one umbrella to help them better coordinate and collaborate to address cyberthreats.

- In 2009, Microsoft Research collaborated with Dartmouth College and the National Center for Missing & Exploited Children (NCMEC) to develop PhotoDNA, an advanced image-matching technology that helps to refine and automate the search for child sex abuse images among the billions of photos on the Internet. NCMEC used the PhotoDNA license to work with online services, such as Facebook, to uncover images of child abuse. Since then, it has become the industry standard for detecting online images of child abuse.

- Microsoft works with NCMEC, INTERPOL, and other organizations to encourage governments to combat child predators.

Policy Considerations

Policymakers can help address the challenges of combating child grooming online by supporting the following efforts:

STRENGTHEN AND ENFORCE EXISTING CHILD PROTECTION LAWS Governments must enact and enforce laws against the sexual exploitation of children, including the possession, production, and distribution of child sex abuse images.

SUPPORT INDUSTRY-WIDE BEST PRACTICES Internet companies should work with governments and law enforcement to help combat online child predation by giving their customers mechanisms for reporting potential predators, enforcing codes of conduct, and spurring further innovation to help reduce illegal or inappropriate content and conduct.

SUPPORT INTERNET SAFETY RESEARCH It is essential that governments commission studies and fund academic and industry research to advance Internet safety. Research is particularly important for identifying factors that increase online risks and for dispelling myths that can lead to misplaced efforts to advance Internet safety.

Combating Human Trafficking Online

Key Points

- Although technology can be used to facilitate the horrific practice of human trafficking, technology can also be used to help combat it.
- Microsoft applies its experience in addressing technology-based crime and invests in research, partnerships, policies, and best practices to support human rights and advance the fight against human trafficking.
- Issues related to human trafficking are complex and require a multi-part solution, including strong public-private partnerships, effective infrastructure for victim support, and intervention efforts founded in solid research.

Human trafficking includes commercial sexual exploitation, forced labor, and other forms of modern-day slavery. Technology can play a role in facilitating—and also combating—these horrific human rights abuses. Although academics are increasingly exploring this area, today there remains insufficient research data to determine the extent to which technology is increasing human trafficking, or the way in which law enforcement and nongovernmental organizations can use technology to better disrupt it.

However, for any intervention efforts to be successful rather than unintentionally cause further harm, it is essential that victims receive the services and support they need when they are recovered from trafficking situations. Assuming that broader systemic progress can be made in ensuring this necessary support for victims, advances in research may lead to future opportunities for effectively using technology to help address trafficking.

Anti-trafficking advocates, law enforcement agencies, and governments around the world have long worked to combat human trafficking. Microsoft believes that technology companies also have an important role to play in driving deeper research and innovation to use technology to more effectively disrupt the business of trafficking people.

Microsoft Approach

Microsoft recognizes its responsibility as a global corporate citizen to respect human rights and aid in the fight against human trafficking. The company expresses its commitment in the human rights statement it released in July 2012 in accordance with the United Nations Guiding Principles on Business and Human Rights.

Microsoft established the Technology and Human Rights Center to help ensure that it meets its commitment to respect human rights. The Center works to advance public understanding of the impact of information and communications technology on human rights. It also aims to coordinate strategic engagement in public policy debates relating to law enforcement, technology, and surveillance to encourage policies that protect human rights.

Microsoft also reflects its commitment to combating human trafficking by investing in research and innovation; establishing partnerships with anti-trafficking advocates and law enforcement agencies worldwide; and implementing policies and best practices to help prevent its technologies from contributing to exploitation.

INVESTING IN RESEARCH AND INNOVATION Microsoft invests in research to develop a more accurate understanding of the role that technology plays in human trafficking, particularly child sex trafficking.

In 2011, Microsoft issued a request for proposals for academic research into the role of technology in the sex trafficking of children. In 2012, the company distributed $185,000 to six winning teams whose research results will be released as they are completed in 2014.

Microsoft Research is collaborating with the Harvard Kennedy School of Government and the University of Southern California Annenberg School on additional related research.

Microsoft works with leading technology institutions and nongovernmental organizations on efforts such as the International Women's Hackathon, which helps foster technology innovation designed to address trafficking.

ESTABLISHING PARTNERSHIPS Microsoft works with anti-trafficking advocates and law enforcement agencies worldwide to help address human trafficking. Through cooperative efforts that raise the cost, risk, and difficulty of doing business for human traffickers, Microsoft can help make it a less lucrative, and therefore less appealing, trade.

Law enforcement, nongovernmental organizations, and other technology companies like Facebook and NetClean use PhotoDNA, an image-matching technology developed by Microsoft and Dartmouth College to help identify images of child abuse.

Microsoft collaborates with the Global Business Coalition Against Trafficking, the White House Office of Science and Technology Policy, the Council on Women and Girls, United Nations Global Initiative to Fight Human Trafficking (UN.GIFT), US state attorneys general, and local police agencies.

As a founding member of the Thorn Technology Task Force, Microsoft collaborates with Facebook, Twitter, Google, and others to explore new ways technology can address the problem of child sex trafficking.

Microsoft supports organizations such as the Polaris Project, International Centre for Missing and Exploited Children (ICMEC), and the International Justice Mission, all of which combat trafficking and support trafficking victims.

IMPLEMENTING POLICIES AND BEST PRACTICES Microsoft works to help prevent its technologies and processes from contributing to exploitation in its operations and those of its suppliers.

All companies doing business with Microsoft must agree to abide by the company's Vendor Code of Conduct, which outlines required ethical business practices, including an explicit prohibition of the use of forced labor.

For its hardware manufacturers and packaging suppliers, Microsoft has invested in a social and environmental accountability program, which includes independent third-party audits to help ensure compliance with its Code of Conduct and local and national regulations. If these standards are not met, suppliers risk remedial action, including termination of their contracts.

Policy Considerations

Governments and policymakers can help address the problem of human trafficking by focusing on the following priorities:

- **CREATE AND ENFORCE STRONG ANTI-TRAFFICKING LEGISLATION** It is vital that governments enact and enforce human trafficking laws that recognize and protect victims while holding traffickers accountable.

- **PROVIDE FUNDING AND INFRASTRUCTURE** Funding and infrastructure for effective victim recovery services is absolutely essential. Without this, any other interventions have the potential to do more harm than good.

- **ENCOURAGE COLLABORATION ON INITIATIVES** Researchers and technology companies should continue to work with governments, law enforcement, and those in the anti-trafficking community to help understand and address the abuses of technology that facilitate trafficking, adopt effective intervention techniques based on research, and develop anti-trafficking initiatives.

Combating Online Bullying

Key Points

- Online bullying has long been a problem; taking it online has opened the door to 24-hour hurt.
- Microsoft promotes efforts to combat online bullying by creating technology tools, enforcing policies against abuse in its online services, providing education and guidance, and establishing partnerships with others.
- Governments play a vital role in helping to combat harassment and threats online through laws that are thoughtfully written, balancing safety and freedom of speech.

Bullying among youth has long been a serious problem. Just like bullying in person, online bullying (also known as *cyberbullying*) is repeated behavior intended to tease, demean, or harass someone less powerful. Young people can bully using any type of Internet-connected device through text and instant messaging, games, or social media such as Facebook and Tumblr. Bullying online opens the door to 24-hour hurt, which can be amplified by anonymity and the potential for broadcast to a wide audience.

There are many reasons why young people mistreat others, whether out of boredom, to get approval or be funny, to retaliate for having been bullied themselves, or because they are in distress. It isn't always intentional—what starts as an argument may escalate. Often, young people may not even recognize their behavior as bullying, rather referring to it as *drama*.[12]

Because young people practically grow up online, it's no surprise that bullying has moved to the Internet. Estimates of the prevalence of online bullying vary. However, in 2012, a Microsoft study of more than 7,500 children ages 8-17 in 25 countries found that 37 percent of those interviewed had experienced meanness online and 24 percent had bullied someone online.[13]

Youth who experience online bullying—whether as one who bullies, who is the target of bullying, or who is a bystander—can suffer damaging mental health consequences. According to the Cyberbullying Research Center, "research reveals a link between online bullying and low self-esteem, family and academic problems, school violence, and delinquent behavior."

Two challenges make stopping online bullying difficult. First, many do not regard it as a serious form of aggression. And second, cyberbullying incidents can slip through the cracks. The Cyberbullying Research Center reports that, "Parents often say that they don't have the technical skills to keep up with their kids' online behavior; teachers are afraid to intervene in behaviors that often occur away from school; and law enforcement is hesitant to get involved unless there is clear evidence of a crime or a significant threat to someone's physical safety."[14]

To address online bullying, everyone—youth, parents, educators and counselors, law enforcement, technology companies, and the community at large—must together create an environment where young people feel comfortable talking with adults about this problem, safe enough as bystanders to get involved, and confident that meaningful steps will be taken to resolve it.

---

12 The Drama! Teen Conflict, Gossip, and Bullying in Networked Publics: **aka.ms/teen_drama**
13 Online Bullying Among Youth 8-17 Worldwide: **aka.ms/OBResearch**
14 Cyberbullying Identification, Prevention, and Response, Cyberbullying Research Center: **www.cyberbullying.us/Cyberbullying_Identification_Prevention_Response_Fact_Sheet.pdf**

Microsoft Approach

CREATING TECHNOLOGY TOOLS Microsoft provides technology tools that can be tailored to each child. Parent can monitor their children's web activity and block unwanted contact using Family Safety on Windows 7 and Windows 8 or monitor kids' phone use in Kid's Corner on Windows Phone. For young gamers, parents can use Online Safety Settings for Xbox Live to specify what activities children can participate in, who they can communicate with, and who can see their profile.

ESTABLISHING INTERNAL POLICIES AND PRACTICES Microsoft enforces policies against abuse and harassment on its online services—for example, through the Code of Conduct on Xbox Live—and moderates content and interactions to address any abuse, illegal activity, or inappropriate material. Customers who misuse Microsoft services are subject to account termination; serious incidents may be reported to law enforcement.

PROVIDING EDUCATION AND GUIDANCE Microsoft produces educational materials for teachers and parents to teach young people how to stand up to online bullying, what to do if a child is involved in it, and how to promote a culture of kindness, which research shows to be a potent way to help stop bullying.

PARTNERING WITH OTHERS Microsoft works with governments, industry groups, and others to help address online bullying through efforts like GetNetWise in the United States and Insafe in the European Union.

Policy Considerations

BALANCE ANTI-HARASSMENT LEGISLATION WITH FREE SPEECH RIGHTS Governments play a vital role in helping to combat online harassment and threats through laws that are thoughtfully written to balance safety and freedom of speech.

PROMOTE COMPREHENSIVE ONLINE SAFETY EDUCATION IN SCHOOLS Government support for anti-bullying education, as part of a comprehensive online safety curriculum for elementary and secondary school students, can provide a foundation for addressing the problem of online bullying. One example of such support is a US law mandating that anti-bullying measures be taught in any school that receives E-Rate funding from the Federal Communications Commission (FCC). (The E-Rate program gives schools and libraries discounts for telecommunications and Internet access.[15])

ENCOURAGE INDUSTRY COOPERATION Microsoft supports legislation that releases access providers from liability for obscene material or abusive behavior if they have made a good-faith effort to screen their services or provided screening devices for parents. Examples include Section 230 of the US Communications Decency Act and the European Union Directive 2000/31/EC.

15 *Laws Require Internet Safety Education in Schools that Receive E-Rate Funds:* www.safeschools.info/bullying-prevention/bullying-prevention-news/362-laws-require-internet-safety-education-in-schools-that-receive-e-rate-funds

Combating Online Fraud

Key Points

- Online fraud is a significant global problem, victimizing millions of unsuspecting consumers each year. In the United States alone, the FBI's Internet Crime Complaint Center recorded just under 300,000 fraud complaints in 2012 with an adjusted dollar loss of US$525 billion.
- Microsoft takes a four-part approach to combating online fraud: dedicating internal teams to fighting cybercrime; developing technology tools; producing education and guidance; and promoting relationships with government, industry, law enforcement, and others.
- Microsoft supports government efforts to fight online fraud through international cooperation, public-private partnerships, and strong enforcement of anti-fraud laws.

The Internet has transformed commerce around the world, building new companies and services and enabling consumers to engage in a wide variety of economic activities. Total global e-commerce sales were projected to exceed US$1.2 trillion in 2013.

However, as economic activity moves increasingly online, so has the problem of fraud, which threatens to undermine the public trust in the benefits of e-commerce. Online fraud is a significant global problem. In the United States alone, the FBI's Internet Crime Complaint Center recorded just under 300,000 fraud complaints in 2012, with an adjusted loss of US$525 billion.

Organized cybercriminals go to great lengths to execute their online schemes in order to steal identities or carry out financial fraud. Criminals lure their victims using such devious tactics as social engineering, phishing, malicious software (or *malware*), and more.

Social engineering takes advantage of people's trust by tricking them into actions such as installing malware disguised as a legitimate app or entering sensitive personal information on a convincing but fake website—actions that can compromise their devices and data.

Phishing scams use email, text, social network messages, or even phone messages that appear to come from a reputable organization; they aim to entice victims to disclose sensitive information, such as account numbers or passwords. In its most recent account, the Anti-Phishing Working Group reported almost 280,000 unique phishing attacks worldwide between June 2012 and June 2013, with the number of brands exploited by phishers at an all-time high.

To combat online fraud successfully, businesses, government, nongovernmental organizations, and consumers worldwide must work together.

Microsoft Approach

DEDICATED INTERNAL TEAMS The Microsoft Digital Crimes Unit is an international legal and technical team working with partners on such issues as malware and intellectual property (IP) crimes as well as technology-facilitated child exploitation. The team applies its legal and technical expertise to help enhance cloud security and create a safer digital world.

With the opening of the Cybercrime Center in late 2013, Microsoft brought its cybercrime experts from the areas of IP crime, botnets, malware, and child exploitation together under one umbrella. When crimes cross these focus areas—as is happening with greater frequency (for example, the Nitol and Citadel botnets)—Microsoft experts can better coordinate and work together to address cyberthreats. The combined team includes more than 100 attorneys, investigators, business professionals, and forensic analysts based around the world.

TECHNOLOGY TOOLS Microsoft offers many tools to help consumers fight online fraud:

- Microsoft Security Essentials is a free program that provides real-time protection against viruses, spyware, and other malware.
- The SmartScreen Filter is a feature in Internet Explorer that helps warn consumers about potential phishing websites and helps protect against the installation of malware. SmartScreen antispam filters are built into Microsoft email programs to help protect customers from messages that may contain fraudulent solicitations.
- The Microsoft Malicious Software Removal Tool checks computers running the most recent versions of Windows for specific malware and then helps remove any infections it finds.
- The Microsoft Safety Scanner is a free tool that provides on-demand scanning and helps remove malware.

EDUCATION AND GUIDANCE The Microsoft Safety & Security Center offers advice to help consumers protect themselves against online fraud, including tips on how to recognize phishing scams and protect against identity theft.

PARTNERSHIPS Microsoft works with many organizations dedicated to fighting online fraud, including the Anti-Phishing Working Group and the National Cyber Security Alliance.

Policy Considerations

Governments can aid in fighting Internet fraud and other cybercrime by supporting the following efforts:

SUPPORT ADOPTION OF 2001 COUNCIL OF EUROPE CONVENTION ON CYBERCRIME Microsoft has joined with industry to encourage countries to adopt and ratify the 2001 Council of Europe Convention on Cybercrime,[16] which requires signatories to adopt and update laws and procedures to address online crime.

BALANCE REGULATION WITH INNOVATION Although it is essential to enact laws against online fraud and enforce the prosecution of cybercriminals, anti-fraud legislation must be carefully crafted so as not to discourage innovation and technology adoption in the process.

ENCOURAGE PUBLIC-PRIVATE PARTNERSHIPS Public and private relationships are essential to addressing the increasing complexities of cybercrime. For example, Microsoft gives technical training to law enforcement agencies worldwide, develops new technologies to combat cybercrime, and has helped protect consumers by taking legal action.

16 *Convention on Cybercrime, 2001:* conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Safer Online Gaming

Key Points

- Online gaming offers a wide variety of content for many audiences, but not all games and apps are appropriate for everyone. Concerns about harmful effects can be addressed through parental involvement and family education, along with such industry rating systems as ESRB, PEGI, and CERO.

- The Microsoft approach to safer, more trusted gaming experiences includes creating technology tools; providing education and guidance; developing internal policies and practices for moderating content and addressing online abuse; and partnering with government, industry, law enforcement, and others.

- The combination of voluntary industry rating systems, family education, and parental involvement offers the best solutions for making informed decisions about game content.

Gaming, whether on a gaming console, tablet, or mobile phone, offers a wide variety of content for many audiences. However, not all games and apps are appropriate for (or acceptable to) everyone, and many people have expressed concern about their potential harmful effects on children. Some governments have responded to these concerns by restricting access to or even banning certain video games because of sexually explicit or violent content.

The gaming industry has taken the initiative by adopting voluntary rating systems. These include the Entertainment Software Ratings Board (ESRB) ratings in the United States, the Pan European Game Information (PEGI) ratings in more than 28 European countries and Israel, and the Computer Entertainment Rating Organization (CERO) in Japan. The industry recognizes that additional tools are needed to help inform consumers. In response, an international working group that includes Microsoft is developing the International Alliance for Rating Content (IARC), a global ratings framework that will enable game developers to apply in one place for game ratings for many rating systems.

These widely recognized rating systems provide descriptive information about game content, which merchants are encouraged to display and which parents can use as a guide to help inform their content decisions. A 2012 report found that one of every two European consumers recognize PEGI labels,[17] and a 2013 ESRB survey found that 75 percent of US parents "regularly check a game's rating before making a purchase."[18] A "secret shopper" program by the US Federal Trade Commission (FTC) in 2013 found that 87 percent of US merchants refused to sell games with a mature rating to a minor.[19]

No matter what games and apps a family decides are suitable, it is vital that parents take an active interest in and understand the ever-changing digital world that captivates children's attention and imagination. Parents should decide what content—be it game, app, music, movie, or television show—is appropriate for their family, and then take the steps they need to set limits based on those choices. To do this, parents must understand the rating systems and technology tools like family safety settings that can help them set those limits.

17 Pan European Game Information (PEGI) Annual Report 2012: **www.pegi.info/en/index/id/1068/nid/media/pdf/390.pdf**
18 ESRB Survey: Parental Awareness, Use & Satisfaction: **www.esrb.org/about/awareness.jsp**
19 FTC Undercover Shopper Survey, March 25, 2013: **www.ftc.gov/news-events/press-releases/2013/03/ftc-undercover-shopper-survey-entertainment-ratings-enforcement**

Microsoft Approach

The Microsoft approach to encouraging more trusted gaming experiences includes creating technology tools, providing guidance, developing internal policies and practices for moderating content and addressing online abuse, and collaboration.

CREATING TECHNOLOGY TOOLS

- Xbox 360 Family Settings enable parents to set and enforce content ratings for games, movies, and television shows; set a pass code to restrict who can change these settings; and set limits on console play time using the family timer.

- On Xbox One, parents use Family and Online Safety controls to specify a maximum age that maps to game ratings. Parents can then decide whether they want Xbox One to always block content that exceeds this rating or make that decision on a case-by-case basis.

- Online Safety Settings for Xbox Live enable parents to create individual profiles that are appropriate for each child's age and maturity. Parents can specify what activities children can participate in (such as multiplayer gaming, video chat, text messaging, or voice messaging), who they can communicate with, and who can see the child's profile or friends list. In addition, Xbox Live supports a reputation system that encourages healthy participation in games while diminishing the reputation of troublemakers and cheaters.

- Windows Phone 8 offers two ways to manage the access of young people to games and apps.

    - Young people under age 18 who have their own Windows Phone sign in with a child's account. They won't be able to download anything until parents set up My Family and add the young person. Once that's done, parents can manage the apps and games that the young person can download from the Windows Phone Store and use the game-rating filter to limit access.

    - For younger ones, parents can use Kid's Corner to create a space on their phone where children can play games, use apps, listen to music, and watch videos that parents have selected.

PROVIDING EDUCATION AND GUIDANCE The work of Microsoft is incomplete if consumers do not know how to use the technology and other resources that are available to help protect young gamers. Microsoft provides educational materials in the Microsoft Safety & Security Center and in the Xbox Live Healthy Gaming Guide.

DEVELOPING INTERNAL POLICIES AND PRACTICES Microsoft develops company-wide policies, standards, and procedures for its products and services that connect with the Internet. The company enforces a code of conduct for users of its gaming services like Xbox Live, and moderates content and interactions to help address any abuse, illegal activity, or inappropriate material.

PARTNERING WITH NONGOVERNMENTAL ORGANIZATIONS, INDUSTRY, AND GOVERNMENT Creating a safer gaming environment requires a holistic approach in which safety advocacy groups, government leaders, and technology providers all play vital roles. Central to Microsoft efforts is engaging—through public policy—with governments around the world and with organizations such as the National Cyber Security Alliance and the Family Online Safety Institute.

Policy Considerations

Government and industry policymakers can help improve safety in online gaming by supporting the following efforts:

ENCOURAGE RATING SYSTEMS AND PARENTAL INVOLVEMENT INSTEAD OF MANDATORY COMPLIANCE The combination of voluntary industry rating systems, family guidance, and parental involvement provides the best solutions for addressing concerns about gaming and other online entertainment. Microsoft also supplies funding and technical expertise in the development of IARC, a best practice that is supported by nongovernmental organizations and rating agencies, both national and independent.

PROMOTE INNOVATION AND CONSUMER EDUCATION In a vibrant ecosystem, game and app developers and publishers should be able to create products and content for customers of all ages. At the same time, these technology businesses must give parents and caregivers the information and tools they need to make informed decisions about the quality and appropriateness of the interactive games and apps that their children play and use.

Online Reputation

Key Points

- Managing an online reputation is important—it can have a significant impact on a person's life in a number of ways, including employment prospects, relationships, and college admissions.
- Microsoft helps its customers cultivate and protect their online reputations by offering relevant education and guidance, establishing internal policies that help customers better manage their content, and creating technology tools.
- Governments must balance the obligation to help citizens protect their online reputations with the right of free expression.

Worldwide, people are living more of their lives online than ever before. It's where many go to promote themselves, spend time with friends, and find employment, education—even a spouse. A 2012 survey of 19,000 respondents in the United States who had married between 2005 and 2012 found that a third had met online.[20] Research in 2013 by the Dutch dating site, Meetic, found that one in five in the Netherlands was in a long-term relationship that had originated online.[21] Since 2010, nearly three-quarters of US job seekers have used the Internet to find employment.

Research also shows that the information that appears about an individual online can have a significant impact on that person's prospects for employment and education. Microsoft research[22] in 2009 found that 70 percent of US hiring managers and 41 percent of UK hiring managers had rejected a candidate because of information found online. A 2012 survey[23] found that 35 percent of admissions officers in the United States "discovered something that negatively impacted an applicant's chances of getting into the school."

Because a simple online search can reveal a great deal about a person, there is increasing interest in online reputation, and in particular, one's digital footprint—the trail left by online activities such as blogging, posting comments or pictures, gaming, and social networking. While a positive digital footprint can enhance a person's employment opportunities and other prospects, a negative one caused by inappropriate photographs or rude comments left online can damage those possibilities. Users of social networking services may reveal details about their lives that are more lasting and available to a wider audience than they may realize, with consequences for their reputations that they may not imagine. It is essential then for consumers to understand the risks and take appropriate steps to protect their reputations.

In 2011, a Microsoft survey[24] of 5,000 adults and children in Canada, Germany, Ireland, Spain, and the United States found that 90 percent have done something to manage their online profile, but only 44 percent actively think about the long-term consequences that their activities have on their online reputation.

20 Marital satisfaction and break-ups differ across on-line and off-line meeting venues. John Caioppo, et. al., University of Chicago, December 2012: **www.pnas.org/content/early/2013/05/31/1222447110**

21 Research on the dating market in The Netherlands: **www.datinginsider.nl/research-on-dating-market-in-the-netherlands-more-than-20-had-a-relationship-that-started-online**

22 Online Reputation in a Connected World, 2009: **www.microsoft.com/security/resources/research.aspx#reputation**

23 Kaplan Test Prep's 2012 Survey of College Admissions Officers: **press.kaptest.com/research-and-surveys/kaplan-test-preps-2012-survey-of- college-admissions-officers**

24 Online Reputation Management: Parents and Children 8-17, 2011: **www.microsoft.com/security/resources/research.aspx#onlinerep**

Microsoft Approach

PROVIDING EDUCATION AND GUIDANCE The Microsoft Safety & Security Center offers advice to consumers on how they can cultivate and protect their online reputations, safeguard their privacy, and avoid, block, and report inappropriate behavior.

ESTABLISHING CONTENT MANAGEMENT POLICIES Microsoft has established content management policies on its sites:

- The Microsoft Terms of Use do not allow customers to "publish, post, upload, distribute or disseminate any inappropriate, profane, defamatory, obscene, indecent or unlawful ... materials," or to "defame, abuse, harass, stalk, threaten or otherwise violate the legal rights ... of others."
- The Microsoft Services Agreement states that "Microsoft may remove your content without asking you if we determine it's in violation of this agreement or the law."

CREATING TECHNOLOGY TOOLS Microsoft offers features that help customers manage their digital footprint in its products and services.

- The Microsoft Personal Data Dashboard—a central location for personal information associated with selected Microsoft products —helps customers control how that information is displayed.
- Internet Explorer offers settings to help people manage their privacy online, including InPrivate browsing. People who use this feature browse as usual, but when they close Internet Explorer, InPrivate deletes passwords, search history, webpage history, and other data.
- The Smart Match feature in Xbox Live matches players in part based on their reputation, reducing the impact that misconduct has on the Xbox Live community.

Policy Considerations

BALANCE REGULATION WITH FREEDOM OF EXPRESSION In crafting legislation, governments must balance the obligation to help citizens protect their online reputations with the right of free expression.

SUPPORT INDUSTRY-LED EDUCATION AND GUIDANCE Technology companies can help their customers cultivate and protect their online reputations by offering relevant education and guidance and by creating policies that help people better manage their content and privacy.

ENCOURAGE INTERNET INDUSTRY COOPERATION Policymakers should support legislation that releases access providers from liability for obscene material or abusive behavior if they have made a good-faith effort to screen their services or provided screening devices for parents. Examples include Section 230 of the US Communications Decency Act and the European Union Directive 2000/31/EC.

Online Safety for Mobile Devices

Key Points

- As the wireless economy expands, so do incentives for (and risks created by) cybercriminals who use malware to steal identities, money, and business data.
- To reduce the risk on mobile devices and help create safer, more trusted mobile computing experiences, Microsoft develops technology tools; provides education and guidance; and partners with government, industry, law enforcement, and nonprofit organizations.
- As governments address the risks of emerging technologies, they must avoid top-down regulation that stymies technology adoption and preserve flexibility so that industry can innovate. In addition, government and industry must collaborate to support and promote mobile safety education for people of all ages.

Mobility is the cornerstone of the twenty-first century connected world, and mobile devices are ubiquitous, fueled by their power, convenience, and always-on connectivity.

For example, 91 percent of all the people on earth have a mobile phone (up from 83 percent in just two years)—more than half (56 percent) of those have a smartphone.[25] In fact, in its Visual Networking Index,[26] Cisco predicts that by 2014 there will be more mobile-connected devices in the world than there are people.

Usage of mobile devices is also expanding. Today, 60 percent of mobile web users worldwide use their mobile device as the primary or exclusive means of going online, and Cisco anticipates that mobile data traffic will grow more than 11-fold between 2013 and 2018.

However, as the wireless economy expands, so do incentives for (and threats from) cybercriminals, whose ultimate goal is to profit from spying on users. According to the *Kaspersky Security Bulletin 2013*,[27] mobile malicious software is one of the fastest-developing IT security risks, doubling in the first six months of 2013.

People's mobile devices hold tremendous amounts of personal (and often business) data, and criminal activity puts these at risk through malware that is designed especially to steal sensitive data from mobile devices, theft of the device itself, or use of unsecured wireless networks to send sensitive information. Mobile botnets are especially destructive because mobile devices are almost always on, so they're reliably available for new instructions from the botnet controller.

Mobile users may suffer identity theft and financial loss. Businesses also stand to lose customer data and intellectual property if personal mobile devices (including flash drives) are used at work and not adequately protected. In addition, personal privacy can be compromised if the location-based data on a mobile device—collected through its GPS or nearby Wi-Fi access points and cell towers—is shared publicly.

Industry invests in innovative solutions to protect device firmware and software from attack. Consumers can also protect themselves and their devices by taking simple steps, so the need is greater than ever for safety training.

Microsoft Approach

DEVELOPING TECHNOLOGY TOOLS Microsoft builds in technology to help protect the data and privacy of mobile users:

25 Infographic: 2013 Mobile Growth Statistics: **www.digitalbuzzblog.com/infographic-2013-mobile-growth-statistics/**
26 Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018: **www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html**
27 Kaspersky Security Bulletin 2013: **www.securelist.com/en/analysis/204792318/Kaspersky_Security_Bulletin_2013_Overall_statistics_for_2013**

- Windows Defender helps guard tablets and laptops against all kinds of malware in real time, and Windows SmartScreen helps warn consumers about potential phishing websites. Parents can use the Family Safety feature in Windows to create a separate account for each family member, enabling them to monitor children online and set specific activity limits.

- Internet Explorer offers settings, including InPrivate browsing, that help users manage their privacy online. People using this feature browse as usual, but when they close Internet Explorer, InPrivate deletes passwords, search history, webpage history, and other data.

- Through the Windows Phone Store, Microsoft works with mobile service providers and independent software companies to give consumers reputable mobile safety apps that can block web-based threats, provide contact management for children, and more. Windows Phone also offers Kid's Corner, where parents can set limits on access to apps, games, and music.

- Windows Phone apps that use location data are required to give customers the ability to turn off that app's access to an individual's location. The Windows Phone location service does not store any unique device identifiers or data that personally identifies users or that would allow tracking or creation of the location history of a device.

PROVIDING EDUCATION AND GUIDANCE The Microsoft Safety & Security Center offers advice on how to use devices more safely, which includes locking phones with PINs or strong passwords, guidance for safe use of public Wi-Fi hotspots and location-based features, and specific advice for kids.

ESTABLISHING PARTNERSHIPS Building greater safety and security requires a holistic approach in which government leaders, law enforcement, technology providers, and nongovernmental organizations collaborate. Microsoft works with industry and others through such organizations as the GSM Association and CTIA–The Wireless Association.

Policy Considerations

SUPPORT FLEXIBLE, BALANCED LEGISLATION THAT ALLOWS FOR INNOVATION As governments address risks associated with emerging technologies and online services, they must also avoid top-down regulation that stymies technology adoption, and preserve flexibility so that industry can innovate. In addition, government and industry must collaborate to establish mobile safety principles to help build a more secure Internet.

ENCOURAGE INDUSTRY BEST PRACTICES AND GUIDELINES Mobile providers should establish voluntary guidelines and best practices that address such issues as content classification, location-based services, and mobile commerce in order to help people make informed decisions about their safety.

SUPPORT COMPREHENSIVE MOBILE SAFETY EDUCATION Governments must work with information and communications providers, online safety organizations, and school districts to provide mobile safety education for consumer and business users, and to promote safety curricula that addresses mobile safety for young people.

Safer Social Networking

Key Points

- Social networks are highly popular and offer enriching experiences, but they may involve such risks as exposure to malicious software, potential loss of privacy, harassment, online bullying, and damage to one's reputation.

- The Microsoft approach to helping people manage their safety and privacy on social networks includes creating technology tools; providing education and guidance; developing internal policies and practices for moderating content and addressing online abuses; and partnering with government, the technology industry, nongovernmental organizations, and others.

- Governments should continue to work with industry to encourage the benefits and mitigate the risks involved in online social networks by jointly establishing industry best practices and guidelines.

Since its early years, the web has undergone a dramatic transformation from largely static webpages to a dynamic, interactive set of web communities. People socialize with their friends on Facebook, Weibo, or Instagram; connect with their colleagues on LinkedIn; explore a virtual world like Second Life; post updates on Twitter; and play games on Xbox Live. Children play on their own social networks like Webkinz or Club Penguin.

The most popular social networks have hundreds of millions of members. Unfortunately, their popularity has also attracted criminals—hackers, spammers, identity thieves, and predators—who misuse the information people disclose to harass, bully, steal identities, and commit fraud. In addition, users of these services may reveal details about their lives that are more lasting and available to a wider audience than they may realize, with consequences for their reputations that they may not imagine. It is essential, therefore, for consumers to understand the risks and take appropriate steps to protect their information, their privacy, and their reputations.

Social networking services raise additional concerns for young people, particularly those under the usual required age of 13, who may use social networks designed for adults. It is important that young people (and their parents and guardians) understand that these sites may contain content inappropriate for children, and that profiles may be viewed by anyone on the Internet. Registering children who are under the required age can violate the terms and conditions of these social sites. Furthermore, young people who are over age 13 but under the age of majority and who lie about their age may bypass protections offered for those under age 18.

Microsoft Approach

Microsoft helps people manage their privacy and safety on social networks through technology tools, education, policies, and partnerships.

CREATING TECHNOLOGY TOOLS

- The Personal Data Dashboard offers a central location for personal information associated with selected Microsoft products and services, and helps you control how it is used by Microsoft. All Microsoft account holders can specify who is able to view their profiles, who can contact them, and who is able to post or view the content they share.

- In Xbox Live, parents can use Online Safety Settings to create individual profiles for each child. This enables them to specify what activities a child can participate in (such as multiplayer gaming, video chat, text messaging, or voice messaging), who they can communicate with, and who can see a child's profile or friends list. In addition, Xbox Live supports a reputation system that rewards healthy participation in games while reducing that of troublemakers and cheaters.

PROVIDING EDUCATION AND ADVICE The Microsoft Safety & Security Center offers guidance on how to use social networks more safely, including those that are location-based, with specific advice for children and teens. Consumers can also find advice on maintaining and restoring their online reputation; suggestions for avoiding online scams; and tips on how to avoid, block, and report inappropriate behavior.

DEVELOPING INTERNAL POLICIES AND practices Microsoft enforces a code of conduct for users of its online services such as Xbox Live, and moderates content and interactions to address illegal activity, inappropriate material, and other abuse.

ESTABLISHING PARTNERSHIPS Creating a safer online environment requires a holistic approach in which government leaders, law enforcement, technology providers, and nongovernmental organizations all play vital roles. Engaging with governments around the world, as well as with organizations like the National Cyber Security Alliance and the Family Online Safety Institute, is central to Microsoft efforts in social networking safety.

Policy Considerations

Policymakers in industry and government can help strengthen the benefits and mitigate the risks involved in online social networks by focusing on these priorities:

- **ESTABLISH AND PROMOTE INDUSTRY BEST PRACTICES** Social networking services should work with governments to establish industry best practices and guidance, such as the Safer Social Networking Principles for the EU.[28] This document "outlines the principles by which social network providers should be guided as they seek to help minimize potential harm to children and young people, and recommends a range of good practice approaches which can help achieve those principles." Microsoft, Facebook, Google, and 15 other technology companies collaborated to develop these principles.

- **PROVIDE FUNDING FOR RESEARCH** Research plays a critical role in identifying the factors that increase risk online and in dispelling myths that can lead to misplaced efforts to address them. Government funding is essential for both academic and industry research in these areas.

- **SUPPORT ONLINE SAFETY EDUCATION IN SCHOOLS** Online safety curricula should become an integral part of schools' efforts to achieve technological literacy for their students, and should include modules that teach digital literacy and civility.

28 *Digital Agenda for Europe:* ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

Internet Security at Work

Key Points

- No business is immune to security threats from cybercriminals. However, there are inexpensive practices that companies can implement to better protect the security of their data, workforce, customers, and networks.

- To help companies work more securely on the Internet and protect company data and financial assets against cyber-crime, Microsoft develops technology tools; provides education and guidance; and partners with government, industry, law enforcement, and nonprofit organizations.

- Governments should work with the private sector to strengthen the security, privacy, and reliability of the cyber-ecosystem. In partnership with the private sector, policymakers should build on industry best practices for risk-based, technology-neutral approaches to mitigating cyberthreats.

No business demographic is immune from cyberattacks. High-profile data breaches of major corporations make big news, giving the impression that cybercriminals are interested in targeting only larger companies. However, according to Symantec, in 2012, attacks directed against businesses with fewer than 250 employees showed the greatest increase.[29]

Financially motivated cybercriminals threaten company intellectual property and bank accounts as well as customer or employee data. Thieves may steal employee credentials to initiate transfers from company bank accounts or take customer data, install malware that appropriates or destroys data, or spy on employees for sensitive data, such as passwords. These can be serious threats because successful crimes could destroy an entire business.

Cybercriminals have many avenues to gain access. They may hack weak passwords, exploit vulnerabilities in software and hardware, break in through a stolen laptop, embed malware on a carelessly used flash drive, or infiltrate through an unsecured wireless network or a device used at a mobile hotspot.

They may also use social engineering tactics like spear phishing. Spear phishers carefully research their marks and send email that appears to come from someone within the company—for example, the head of human resources or a coworker. It may request a user name or password or invite the recipient to click a link, which will install spyware or other malware. Cybercriminals may also break into a company network through inadequately secured personal devices that employees use to access corporate data.

Fortunately, the steps to help defend company assets need not require broad security expertise or great expense. Companies can help protect their assets by taking steps that include the following:

- Setting up a secure system by controlling network access, installing legitimate antimalware software, and keeping software current automatically for all devices (personal and company-owned).

- Protecting business data with regular backups, by encrypting sensitive business information, and through the secure disposal of company equipment.

- Training the workforce to create strong passwords, to be on the alert for scams so as not to be tricked into downloading malware, and to treat all public Wi-Fi networks as a security risk.

- Being prepared by developing security policies, including for personal devices that employees use at work. Businesses also need to be aware of threats outside the business network, and to put practices in place that watch for and correct unexpected payments, data leakage, and other such events.

29 2013 Internet Security Threat Report, Symantec: **www.symantec.com/security_response/publications/threatreport.jsp**

Microsoft Approach

Microsoft seeks to address the problem of online security in the workplace through a combination of technology, education, and collaboration.

DEVELOPING TECHNOLOGY TOOLS Microsoft builds technology to help businesses secure their assets:

WINDOWS UPDATE can be set to automatically download and install updates to Windows as well as to device drivers and other Microsoft software.

MICROSOFT SECURITY ESSENTIALS AND WINDOWS DEFENDER help protect against malware. Microsoft Security Essentials is a free program that provides real-time protection against malware. Windows 8 builds in this protection with Windows Defender (replacing Microsoft Security Essentials).

THE SMARTSCREEN FILTER, a feature in many Microsoft products, helps protect against the installation of malware by warning consumers about potential phishing websites and attacks that use social engineering tactics.

THE MICROSOFT SAFETY SCANNER provides free scanning on demand and helps remove malware.

THE MICROSOFT MALICIOUS SOFTWARE REMOVAL TOOL checks computers using supported versions of Windows for prevalent malware and helps remove any infections it finds.

BITLOCKER DRIVE ENCRYPTION AND ENCRYPTING FILE SYSTEM (EFS) are two data encryption options available to some Windows users. BitLocker Drive Encryption encrypts an entire hard drive, and EFS can be used to encrypt individual files as needed.

WINDOWS INTUNE helps companies manage computers and mobile devices from the cloud, enabling people to use the devices they choose while following corporate policies.

PROVIDING EDUCATION AND GUIDANCE Microsoft created the Internet Security at Work Toolkit expressly to help companies teach their employees how to work more securely online and better defend company, customer, and personal information.

ESTABLISHING PARTNERSHIPS Building greater safety and security requires a holistic approach in which government leaders, law enforcement, technology providers, and nongovernmental organizations work together.

Microsoft collaborates with the National Cyber Security Alliance (NCSA), which helps companies assess their security risks, monitor threats, report cyberattacks, and implement a cybersecurity plan. Microsoft also partners with the US Federal Communications Commission (FCC), Federal Trade Commission (FTC), Department of Homeland Security (DHS), and Chamber of Commerce to build business awareness of their role in keeping their networks and employees safer online.

Policy Considerations

Policymakers in government and industry can help companies work more securely on the Internet and protect company data and financial assets against cybercrime by adhering to the following principles:

- **PROMOTE SECURITY TRAINING FOR EMPLOYEES** Industry must establish voluntary guidelines and best practices for employee security training.

- **BUILD ON EXISTING FRAMEWORKS AND BEST PRACTICES** In partnership with the private sector, policymakers should build on industry best practices for risk-based, technology-neutral approaches to mitigating cyberthreats. When policymakers rely upon tested frameworks, they help ensure that hard-won security gains are maintained and technological innovations are given maximum opportunity to succeed.

- **DEVELOP GLOBALLY HARMONIZED LAWS AND STANDARDS** Conflicting laws can complicate compliance across local, state, provincial, or national borders. The wide variance in rules, regulations, and laws threatens to impede economic progress and stifle innovation. In countries such as the United States with multiple state laws, broad federal preemption must be a part of any comprehensive privacy legislation.

Global Online Safety Partnerships and Initiatives

Key Points

- Creating a safer online environment requires a holistic approach in which consumers, government leaders, technology providers, and nongovernmental organizations collaborate.
- Microsoft efforts have centered on engaging through public policy with governments around the world, with organizations like the National Cyber Security Alliance and the Family Online Safety Institute, and on such online safety initiatives as STOP. THINK. CONNECT.
- Cooperation among all stakeholders—consumers, government, law enforcement agencies, the technology industry, and nonprofit organizations—is one of the most effective means for helping to make the Internet a safer, more secure, and trusted environment.

The Internet may be the landmark invention of this era, offering new ways to work, connect, learn, and play. But, like the real world, the Internet comes with risk. Unfortunately, the digital age has enabled sophisticated new ways of causing harm to people and their property, businesses, and even nation states.

One of the best ways to help protect people online is to make them aware of potential pitfalls and help them develop skills and strategies for avoiding them. This requires a holistic approach in which consumers, government leaders, technology providers, and nongovernmental organizations collaborate.

Microsoft Approach

For decades, Microsoft has invested in consumer awareness about the safer use of technology and the Internet. Microsoft efforts have centered on engaging through public policy with governments around the world, as well as with nongovernmental organizations such as the National Cyber Security Alliance and the Family Online Safety Institute, and on such online safety initiatives as National Cyber Security Awareness Month, Safer Internet Day, and STOP. THINK. CONNECT.

NATIONAL CYBER SECURITY ALLIANCE (NCSA). NCSA is a prime example of a successful partnership that includes the Department of Homeland Security, business, and nonprofit organizations. Microsoft was a founding member, has played a leadership role since NCSA's inception in 2001, and has contributed to the following important NCSA initiatives:

National Cyber Security Awareness Month each October is a program dedicated to raising public awareness of online risks and informing people about how to mitigate them. As a key sponsor and serving on the board, Microsoft contributions have included research, consumer guidance on key online safety and security issues, and participation in special forums and events.

STOP. THINK. CONNECT. is a consumer awareness and education campaign that was launched in October 2010. Its simple message—to stop and think before conducting online activities—reminds people to exercise caution. The campaign, created by an unprecedented coalition of 30 representatives from industry, government and the nonprofit sector, was the result of 16 months of research and testing. It is an important step toward building a unified culture of online safety, similar to public awareness efforts aimed at encouraging seat-belt use and preventing forest fires.

FAMILY ONLINE SAFETY INSTITUTE (FOSI) FOSI is an international nonprofit organization that works to make the online world safer for kids and their families. Microsoft employees have served in a leadership capacity, and the company has participated in its research, events, and special projects to develop innovative solutions and policies in the field of online safety. These efforts include the following:

Support for A Platform for Good, which seeks to promote and encourage digital citizenship among parents, educators, and youth. While recognizing the potential risks, it aims to celebrate technology as a vehicle for opportunity and social change. Microsoft continues to promote the initiative through its blogs and other social media.

Financial support for the Global Resources Information Directory (GRID), a comprehensive directory of online safety information that monitors the efforts of countries around the world to make the Internet safer for their citizens.

Work on the Broadband Responsibility Project to create a checklist for implementing a comprehensive broadband responsibility plan in schools, communities, and states.

SAFER INTERNET DAY Microsoft is a long-standing supporter of Safer Internet Day, a global campaign organized by Insafe and co-founded by the European Union, which promotes more responsible use of online technology and devices. Microsoft helps promote the day, provides supporting research such as the Microsoft Computing Safety Index, and leads and participates in activities that help educate consumers about safer online habits.

Policy Considerations

Policymakers can advance the work of global partnerships and initiatives in making the Internet a safer and trusted environment by focusing on the following:

- **SUPPORT PUBLIC AWARENESS EFFORTS** Governments and companies worldwide should invest jointly in Internet safety by supporting programs aimed at increasing public awareness of Internet risks and guidance to help people avoid them.

- **ENCOURAGE COLLABORATION AND PUBLIC-PRIVATE PARTNERSHIPS** Cooperation among all stakeholders—consumers, government, law enforcement agencies, the technology industry, and nonprofit organizations—is one of the most effective means for helping to make the Internet a safer, more secure, and trusted environment.

- **PROMOTE SELF-REGULATION AND FLEXIBLE LEGISLATION** To better protect people online, industry must regulate itself and government must develop thoughtful legislative frameworks for addressing risk in emerging technology areas. As governments do this, it is essential that they leave room for innovation and flexibility in the process.

- **SUPPORT RESEARCH THROUGH FUNDING** Research plays a critical role in identifying the factors that increase risk online and in dispelling myths that can lead to misplaced efforts to address them. Government funding is essential for both academic and industry research in these areas.

Resources

ONLINE SAFETY

Microsoft Security & Safety Center with online safety guidance: **www.microsoft.com/security**

Online Fraud: Your Guide to Prevention, Detection, and Recovery: **aka.ms/OnlineFraudBooklet**

Microsoft Computing Safety Index (MCSI): **www.microsoft.com/security/resources/mcsi.aspx**

National Cyber Security Alliance: **www.staysafeonline.org**

Family Online Safety Institute (FOSI): **www.fosi.org**

A Platform for Good: **www.aplatformforgood.org**

DIGITAL CITIZENSHIP

Microsoft Digital Citizenship in Action Toolkit: **aka.ms/free_resources**

Fostering Digital Citizenship, Microsoft visual whitepaper: **aka.ms/digitalctz**

Research and curriculum materials promoting digital citizenship: **www.digitalcitizenship.net**

Microsoft Global Online Safety Footprint 2013: **aka.ms/safety_footprint**

Online Safety 3.0: Empowering and Protecting Youth: **aka.ms/Online-Safety30**

The Family Online Safety Institute: **www.fosi.org**

CHILD ONLINE SAFETY

Microsoft Security & Safety Center with age-based guidelines for Internet use:
www.microsoft.com/security

The International Centre of Missing & Exploited Children (ICMEC): **www.icmec.org**

The Family Online Safety Institute: **www.fosi.org**

A Platform for Good: **www.aplatformforgood.org**

A comprehensive directory of parental control tools and safety education guidance:
www.getnetwise.org

ONLINE SAFETY EDUCATION

Fostering Digital Citizenship: **aka.ms/digitalctz**

ThinkUKnow: **www.thinkuknow.co.uk**

Microsoft Global Online Safety Footprint 2013: **aka.ms/safety_footprint**

Microsoft Partners in Learning: **www.pil-network.com**

Microsoft YouthSpark: **aka.ms/youthspark**

European Commission Safer Internet Programme: **aka.ms/EC-SaferInternet**

The Microsoft Safety & Security Center with age-based guidelines for Internet use:
www.microsoft.com/security

Microsoft Digital Citizenship in Action Toolkit: **aka.ms/DC-Toolkit**

National Cyber Security Alliance safety tools and materials:

www.staysafeonline.org/teach-online-safety

FAMILY SAFETY SETTINGS

Microsoft Security & Safety Center safety guidelines for the whole family:

www.microsoft.com/security/family-safety

Comparison of Microsoft family safety tools: **aka.ms/compare-tools**

A Platform for Good: **www.aplatformforgood.org**

A comprehensive directory of parental control tools and safety education:

www.getnetwise.org

MICROSOFT COMPUTING SAFETY INDEX

Microsoft Computing Safety Index (MCSI): **www.microsoft.com/security/resources/mcsi.aspx**

The MCSI survey (abbreviated version): **aka.ms/MCSISurvey**

Online safety research from Microsoft: **www.microsoft.com/security/resources/research-studies.aspx**

COMBATING CHILD EXPLOITATION ONLINE

Microsoft PhotoDNA: **www.microsoftphotodna.com**

The Microsoft Digital Crimes Unit: **www.microsoft.com/DCU**

Microsoft Cybercrime Center: **aka.ms/cybercrime-center**

Thorn: Digital Defenders of Children: **www.wearethorn.org**

Microsoft human rights statement: **aka.ms/Human-Rights-Statement**

The National Center for Missing & Exploited Children (NCMEC): **www.ncmec.org**

Microsoft research initiative on the role of technology in human trafficking:

aka.ms/human-trafficking-rfp

COMBATING CHILD GROOMING ONLINE

Microsoft PhotoDNA: **www.microsoftphotodna.com**

The Microsoft Digital Crimes Unit: **www.microsoft.com/DCU**

Microsoft human rights statement: **aka.ms/Human-Rights-Statement**

The National Center for Missing & Exploited Children: **www.ncmec.org**

COMBATING HUMAN TRAFFICKING ONLINE

Microsoft Technology and Human Rights Center: **aka.ms/Technology_Human_Rights**

Microsoft human rights statement: **aka.ms/Human-Rights-Statement**

Global Business Coalition Against Trafficking: **www.gbcat.org**

Polaris Project: **www.polarisproject.org**

International Centre for Missing and Exploited Children (ICMEC): **www.icmec.org**

Thorn: Digital Defenders of Children: **www.wearethorn.org**

Microsoft Research: **research.microsoft.com**

Microsoft PhotoDNA: **www.microsoftphotodna.com**

Microsoft research initiative on the role of technology in human trafficking: **aka.ms/human-trafficking-rfp**

COMBATING ONLINE BULLYING

Microsoft Safety & Security Center materials to help adults and young people stand up to online bullying: **www.microsoft.com/security/family-safety/online-bullying.aspx**

A comprehensive directory of parental control tools and safety education: **www.getnetwise.org**

Cyberbullying Research Center: **www.cyberbullying.us**

An online safety education site that Microsoft created in cooperation with the European Union: **www.saferinternet.org**

Resources to help address bullying in the United Kingdom: **www.bullying.co.uk**

Wired Safety: **www.wiredsafety.org**

COMBATING ONLINE FRAUD

Online Fraud: Your Guide to Prevention, Detection, and Recovery: **aka.ms/OnlineFraudBooklet**

The Microsoft Digital Crimes Unit: **www.microsoft.com/dcu**

Microsoft Cybercrime Center: **aka.ms/cybercrime-center**

Malicious Software Removal Tool: **aka.ms/msrt**

Microsoft Safety Scanner: **aka.ms/scanner**

The Microsoft Safety & Security Center with antifraud guidance for consumers: **www.microsoft.com/security/online-privacy**

SAFER ONLINE GAMING

The Xbox Live Code of Conduct: **aka.ms/XboxLive_COC**

Family Safety on the Microsoft Safety & Security Center: **www.microsoft.com/security**

Xbox Live Healthy Gaming Guide: **www.xbox.com/en-US/live/healthygamingguide**

Entertainment Software Ratings Board: **www.esrb.org**

Pan European Game Information: **www.pegi.info**

Computer Entertainment Rating Organization: **www.cero.gr.jp**

ONLINE REPUTATION

Microsoft Services Agreement: **aka.ms/services-agreement**

Microsoft Privacy Settings: **www.microsoft.com/security/online-privacy/overview.aspx**

Microsoft Personal Data Dashboard: **aka.ms/dashboard**

Microsoft Safety & Security Center: Take charge of your online reputation: **aka.ms/reputation**

ONLINE SAFETY FOR MOBILE DEVICES

Microsoft Security & Safety Center with mobile safety advice: **www.microsoft.com/security**

Microsoft advice on safer use of location-based services: **aka.ms/location_safety**

Privacy and location services on Windows Phone: **aka.ms/location-privacy**

CTIA–The Wireless Association: **www.ctia.org**

GSM Association: **www.gsma.com**

Coalition of mobile providers in the United Kingdom promoting social responsibility in the mobile phone industry: **www.mobilebroadbandgroup.com**

SAFER SOCIAL NETWORKING

The Microsoft Safety & Security Center guidance: **www.microsoft.com/security**

National Cyber Security Alliance: **www.staysafeonline.org**

The Family Online Safety Institute: **www.fosi.org**

STOP. THINK. CONNECT. Online safety tips and advice: **www.stopthinkconnect.org**

INTERNET SECURITY AT WORK

Internet Security at Work Toolkit:
www.microsoft.com/security/resources/teach-others-work.aspx

Microsoft guidance for defending computers: **www.microsoft.com/security/pypc.aspx**

FCC Small Biz Cyber Planner 2.0: **www.fcc.gov/cyberplanner**

U.S. Department of Homeland Security Cybersecurity: **www.dhs.gov/topic/cybersecurity**

National Cyber Security Alliance: **www.staysafeonline.org/business-safe-online**

U.S. Chamber of Commerce Internet Security Essentials for Business 2.0:
aka.ms/USCC_biz_security

GLOBAL ONLINE SAFETY PARTNERSHIPS AND INITIATIVES

Microsoft Safety & Security Center: **www.microsoft.com/security**

National Cyber Security Alliance: **www.staysafeonline.org**

National Cyber Security Awareness Month: **www.staysafeonline.org/ncsam**

Safer Internet Day: **www.microsoft.com/security/resources/sid.aspx**

STOP. THINK. CONNECT.: **www.stopthinkconnect.org**

Family Online Safety Institute: **www.fosi.org**

A Platform for Good: **www.aplatformforgood.org**

Global Resources Information Directory (GRID): **www.fosigrid.org**

Microsoft Computing Safety Index: **www.microsoft.com/security/resources/mcsi.aspx**

Microsoft

Accessibility

Building Global Trust Online, 4th Edition

Microsoft Perspectives for Policymakers

Who Benefits from Accessible Technology

— and How Great Is the Need?

THERE ARE
~1 BILLION PEOPLE
with disabilities worldwide

THAT'S **15%** of the global population[1]

OF THOSE BILLION, NEARLY 20%
(~200 million) have severe disabilities[2]

And everyone can benefit from assistive technology[3]

Types of disabilities and impairments

VISUAL — **285 MILLION PEOPLE** *worldwide (4%) have a vision impairment*

39 MILLION are blind
246 MILLION have low vision[4]

HEARING — **360 MILLION PEOPLE** *worldwide (5%) are deaf or hard of hearing*[5]

SPEECH

6-8 MILLION AMERICANS
(2-3%) have some difficulty understanding or using language[6]

DEXTERITY

ABOUT 2.9 MILLION PEOPLE IN THE UK
(24% of disabled people) have a dexterity disability[7]

COGNITIVE/ INTELLECTUAL

15.2 MILLION AMERICANS
ages 15+ (5%) have a cognitive or intellectual disability[8]

Accessible technology can also benefit people with situational disabilities who are:

Struggling to hear a call in a noisy airport or restaurant

Unable to read small text on a device

Using a mouse or keyboard in a tight space

Read on to learn more about the need for accessible technology

[1] World Report on Disability. World Health Organization and The World Bank, 2011. whqlibdoc.who.int/publications/2011/9789240685215_eng.pdf | [2] ibid | [3] www.gartner.com/newsroom/id/2638315 | [4] www.who.int/mediacentre/factsheets/fs282/en | [5] www.who.int/mediacentre/factsheets/fs300/en/index.html | [6] www.nidcd.nih.gov/health/statistics/pages/vsl.aspx | [7] Family Resources Survey 2011/12. United Kingdom. www.gov.uk/government/publications/family-resources-survey-201112 | [8] www.cdc.gov/aging/pdf/cognitive_impairment/cogimp_poilicy_final.pdf

Accessibility

Key Points

- Accessibility features make it easier for everyone to use technology and to personalize their computers to meet their needs and preferences.
- For many people who live with physical or cognitive disabilities, accessibility features are what make computer use possible.
- Microsoft is committed to developing innovative accessibility solutions through four key areas of focus: product accessibility, leadership and awareness, innovation, and collaboration.
- Policymakers can support accessibility by enacting policies that promote people-centric design; pointing to voluntary, technology-neutral industry standards; and letting the market-place determine the best balance of built-in features, services, and third-party technologies.

As technology becomes increasingly important in day-to-day living—for work, commerce, and communication—it is vital that everyone, regardless of ability or age, be able to enjoy the benefits of the digital world. Accessible technology enables people to personalize the settings on their computers and other devices to make them easier to use.

For many people with physical or cognitive impairments, accessibility features are what make computer use possible. For example, adjustable display settings and text-to-speech features benefit people who have low vision. Hands-free technology benefits those with mobility impairments who have difficulty using a keyboard or a mouse. Simplified visual displays and picture-to-speech features can make computer use easier for people who have cognitive impairments.

Accessible technology is also helpful to those who want to customize their computing experience to address temporary situational needs, such as a noisy environment or bright sunlight.

In addition to built-in accessibility options that let people personalize their computer settings, accessible technologies also include assistive products, such as screen readers, magnifiers, and specialty keyboards. Innovative hardware and software products and built-in accessibility settings are essential tools for computer users who have visual, dexterity, speech, and other impairments, as well as those with situational limitations.

Microsoft Approach

Microsoft is committed to developing innovative accessibility solutions through four key areas of focus:

PRODUCT ACCESSIBILITY

LEADERSHIP & AWARENESS

INNOVATION

COLLABORATION

Many Microsoft products have built-in accessibility and personalization options:

WINDOWS 8 works on touch-only devices and offers touch-compatible updates to accessibility features such as Narrator and Magnifier. The Windows 8 Ease of Access Center helps people manage an array of accessibility options.

OFFICE 2013 provides integration with Windows 8 accessibility features and offers other accessibility features, such as Read Mode in Word 2013 and the Accessibility Checker for documents, spreadsheets, and presentations.

OFFICE 365 offers keyboard accessibility and high-contrast modes, and it supports display modes that make the Word Web App and PowerPoint Web App accessible to screen readers.

More than two decades ago, Microsoft began its leadership in the field of accessibility and its commitment to developing innovative accessibility solutions. The company helps raise awareness by providing information about its accessibility offerings—including demos, tutorials, and guides—on the Microsoft Accessibility website and in the Microsoft Accessibility Update newsletter.

Microsoft Accessibility website *Microsoft Accessibility Update newsletter*

Microsoft promotes accessibility innovation in the development community and works with industry organizations to advance accessibility. The Microsoft Accessibility Developer Center provides tools and guidance for developing accessible applications and web content. Microsoft engages in accessibility-related research and development projects, including large-scale nationwide studies and targeted usability studies.

Microsoft collaborates with a wide range of organizations to help raise awareness of the importance of accessible technology. Microsoft has built strong relationships with organizations such as G3ict, UNESCO, Trust for the Americas, and national disability groups in many countries.

Policy Considerations

Governments and policymakers can help encourage the development of accessibility solutions by supporting the following priorities:

- **DEVELOP AND HARMONIZE GLOBAL STANDARDS** Market-led accessibility standards that are globally harmonized—along with procurement policies that reference them—are the foundation of a robust ecosystem of interoperable technologies.
- **ENSURE TECHNOLOGY NEUTRALITY** Technology-neutral policies help promote innovation, help eliminate barriers to trade and market access, encourage enhanced competition, and help prevent bias in government procurement.
- **PROMOTE DIGITAL INCLUSION** Governments should create policies and programs that advance digital inclusion for people with disabilities and older adults—particularly in education, the workplace, and government services.
- **FOCUS ON OUTCOMES** Governments should promote people-centric design by focusing on desired outcomes rather than specific features.
- **SUPPORT INTEROPERABILITY** Interoperability is a key feature of Microsoft accessible technologies. Microsoft advocates public policies that allow for a variety of complementary ways to achieve it. Governments should allow technology vendors and purchasers to choose the solutions that best suit their needs.

Accessibility and People-Centric Design

Key Points

- Advances in technology are enabling more personalized and relevant experiences for users. This approach—known as *people-centric* design—helps everyone, including people with disabilities, use computing devices and services more easily.
- People-centric design greatly expands the ways people can interact with products, services, and devices—to include voice commands, touch, and gestures.
- Microsoft believes that natural user interfaces, machine learning, scenario-based engineering, and other elements of people-centric design will not only expand opportunities for people with disabilities, but will also help a broad range of users who have temporary situational impairments.
- Government policies should encourage market-driven advances in people-centric design that emphasize general outcomes and avoid narrowly prescriptive rules that can hinder innovation.

The technology industry has been investing in new, more natural ways for people to interact with technology. Devices and services are behaving in increasingly intelligent ways by anticipating users' needs, understanding their intentions, and adapting to their immediate surroundings.

This new approach, known as *people-centric design,* includes several key elements:

CONTEXTUAL AWARENESS	Accounting for the user's circumstances in assisting with, automating, or completing tasks.
SENSORY INPUT	Processing natural inputs (such as vision, voice, and gestures) and communicating back to the user in a natural and context-appropriate way.
LANGUAGE AND INTELLIGENCE	Understanding key aspects of natural language, inferring the user's intentions and goals, and engaging in dialogue with the user.
ANTICIPATORY PROCESSING	Factoring in the user's past and concurrent actions and workflow to assist with tasks.
ENVIRONMENTAL AWARENESS	Using data about a device's current and past environments to assist with tasks.
AUGMENTED INTERACTION	Using 3-D, immersive, and telepresence technologies to create the most natural environment for human-computer interaction.
ADAPTIVE BEHAVIOR	Transitioning seamlessly among devices and contexts so the user doesn't have to switch modes manually.

Devices and services that combine all of these attributes can make interacting with a computer easier not only for people with disabilities and those with age-related impairments, but also for those with temporary constraints—such as drivers who cannot safely look at a device screen, or people who are in noisy environments where sounds are difficult to distinguish.

Microsoft Approach

Microsoft believes that the opportunity is ripe for more people-centric innovation in devices and services. Given the right policy landscape, the new interaction paradigms can lead to a cycle of innovation that addresses key concerns for policymakers related to education, employment, public health, and more. These innovations will help expand opportunities for people who have disabilities and will also help a broad range of users who have temporary situational impairments.

Underlying this new wave of innovation is *scenario-based engineering*—a design process that looks at what users want to accomplish in specific situations and builds the technology to address those use scenarios.

Microsoft is committed to engaging with the accessibility community, policymakers, and the technology industry to promote this important trend in digital inclusion and incorporate people-centric design into the devices and services of the future.

Policy Considerations

Policymakers can help foster a regulatory environment that is open to the advantages of people-centric design by adhering to the following principles:

- **FOCUS ON OUTCOMES INSTEAD OF FEATURES** Public policies often designate "disabilities" as a category of needs that engineers should address, and accessibility features are simply added on to technology designed for mainstream users—but most people have needs that fall somewhere in between. Policies should emphasize general outcomes and scenario-based engineering instead of mandating specific features for people with specific disabilities.

- **PROMOTE INTEROPERABILITY AND USER CHOICE** Policies should promote market incentives and interoperable solutions that leave room for older technologies and encourage the development of new ones. Policymakers should avoid defining specific roles and responsibilities for certain industry players, which drives up the cost of developing accessible technologies. They should also avoid mandating or developing unique standards, instead pointing to existing voluntary, market-driven industry standards.

- **EDUCATE CONSUMERS AND THE PUBLIC** Policymakers should encourage education and public discourse about accessible people-centric products and services.

Accessibility and the Cloud

Key Points

- For people with disabilities—including visual, dexterity, cognitive, and speech impairments—access to computing and the Internet starts with a personal device that offers accessibility settings and can customize the user experience.
- Microsoft envisions a world of accessible, connected devices that can understand and interpret users' needs, preferences, and immediate surroundings. This experience, in combination with cloud-based services, will allow preferences to follow users wherever they go and on whatever device they use.
- Policymakers should support existing standards for accessibility and cloud computing that encourage a vibrant, market-driven ecosystem of accessible devices, software, and services.

For people who live with disabilities—more than 1 billion people worldwide, according to a World Health Organization report—the ability to use computers and access the Internet can be crucial to being an active part of the workforce and of society as a whole. At the same time, it has become common for people to own multiple devices and to move among them throughout the day. A 2013 Pew Research Center study found that more than half of American adults have a smartphone and more than a third own a tablet computer. For users with impairments, it is important to have a uniformly accessible experience across all the devices they use.

MORE THAN HALF
of American adults have a smartphone

MORE THAN A THIRD
own a tablet computer

The cloud can be helpful in this respect by serving as a repository of user preferences and settings, and by providing that information to cloud-connected devices. It can also provide a way to sync devices when those settings change. However, the physical device remains the key to delivering a personalized user experience. The device is where technological advances—such as machine learning and natural user interfaces that respond to touch, voice, vision, and gestures—are revolutionizing accessibility. Devices are adapting to, and even anticipating, users' needs.

As the population ages, and as assistive technologies and services become more sophisticated, technology companies must be allowed to continuously innovate and integrate machine learning, natural user interaction, and cloud services to advance digital inclusion.

Microsoft Approach

For more than 25 years, Microsoft has been introducing accessibility features into software products. These include options in the Windows operating system and other products that help users personalize the computer display, mouse, keyboard, and sound and speech settings.

Microsoft has also worked closely with companies that specialize in accessibility products such as:

SCREEN READERS

MAGNIFIERS

SPECIALTY KEYBOARDS

Built-in accessibility features in personal computing devices include those that read text aloud, add captions to video, and allow hands-free entry of information using speech. For example, Microsoft first introduced Windows Speech Recognition in 2006 in Windows Vista. More recently, Microsoft added speech recognition technology to the Kinect motion-sensing device for Xbox. These tools make

hands-free, voice-activated commands possible for users, including those who have temporary injuries, permanent disabilities, or situational limitations that prevent them from using the keyboard or mouse.

These "building blocks" in mobile devices and personal computers foster the growth of a vibrant accessible technology ecosystem. They will also lead to increasingly intuitive and adaptive user interfaces, as well as complex capabilities such as data visualization and real-time simulation of 3-D environments.

Microsoft envisions a world of accessible, connected devices that can understand and interpret users' needs, preferences, and immediate surroundings. This fully adaptive experience, in combination with cloud-based services, will allow preferences to follow users wherever they go and on whatever device they use.

The key characteristics of these next-generation accessible devices include multi-modal interaction (including speech, touch, gesture, and eye gaze), contextual awareness (sensing factors such as ambient noise, lighting level, whether the user is in a car, and the user's mood), and the ability to be personalized for each individual.

In some scenarios, cloud-based tools can be helpful by adapting content, translating between languages, or using crowd-sourced services to improve the accessibility of photos, graphics, or webpages. However, there will continue to be a need for powerful assistive technology within each device in order to provide a consistent experience of the device and all its capabilities.

Policy Considerations

Policymakers can encourage growth of a market-driven accessible technology ecosystem for all users on all devices by focusing on the following priorities:

- **SUPPORT EXISTING ACCESSIBILITY STANDARDS** A healthy market-driven ecosystem of many products, business models, and development approaches is the best environment for encouraging accessibility. Policymakers can help by supporting standards such as ISO/IEC 40500 (W3C Web Content Accessibility Guidelines 2.0), which covers all web-based user interfaces, instead of crafting new ones in response to the growth of cloud computing.

- **SUPPORT GLOBALLY HARMONIZED STANDARDS** The speed of innovation in the technology sector can outpace legislative measures that are meant to encourage accessibility and promote cloud services. Globally harmonized standards are the best way to encourage a broad array of interoperable products—not laws that prescribe specific features or services and exclude others.

- **PROMOTE MARKET INCENTIVES** Policymakers can help reduce the cost of developing accessible technologies by promoting market incentives and a broad ecosystem of interoperable solutions. Policies that favor user choice, technology neutrality, and interoperability will leave room for older technologies while spurring the development of new ones.

- **ENCOURAGE PUBLIC-PRIVATE PARTNERSHIPS** Governments, industry, and consumer advocacy organizations can deliver the greatest benefits to users of all abilities by collaboratively exploring new ways that devices and cloud services can help users with accessibility needs.

Accessibility in Education

Key Points

- More than 100 million children around the world live with a moderate to severe disability, according to some estimates.
- Accessible technologies are helping to expand access to education for children with disabilities, as well as provide new learning and job training opportunities for adults with disabilities.
- Microsoft is dedicated to building accessibility into its products, providing accessibility resources for educators, and advancing model policies that can help guide governments in making education more inclusive for all.

Of the more than 1 billion people worldwide who live with some form of disability, more than 100 million are children, according to a World Health Organization report. Barriers to education for children with disabilities contribute to high rates of unemployment and poverty among adults with disabilities.

Fortunately, accessible technologies are making it easier for all students—including those with vision, hearing, mobility, dexterity, language, and learning impairments—to gain equal access to education as well as acquire technology skills that are important in many jobs and careers. These technologies are also providing new job training opportunities for adults with disabilities.

For example, touch interfaces, word-prediction features, and speech recognition can help students who have dexterity challenges. Adjustable display settings and text-to-speech features can help those with low vision. Technology can also help students with disability-related social challenges by providing opportunities to communicate and collaborate with their peers in new ways.

Microsoft Approach

Microsoft has worked with government agencies, nonprofit organizations, advocacy groups, and industry leaders for more than two decades to advance inclusiveness in education.

The company has identified five key priorities in helping to make education accessible to all:

- **ACCESS TO DIGITAL CONTENT** including e-books, websites, and distance learning programs
- **ACCESSIBLE TECHNOLOGY** products and services, including tools for creating accessible content
- **INCLUSIVE CURRICULA** that consider the needs of all students and facilitate collaboration
- **REASONABLE ACCOMMODATION** for students through accessible technology
- **TRAINING AND INFORMATION** for educators, students, and their families

Microsoft provides a number of educational resources, including accessibility guides for educators, curriculum resources, teacher-training workshops on accessibility, and articles and videos about how students with disabilities are using technology to enhance their learning.

Microsoft also supports the development of model policies that can help guide governments in making education more inclusive. One example is the Model Policy for Inclusive Information and Communication Technologies (ICT) in Education, which was jointly developed by UNESCO and G3ict in 2013. This document supports educational practices that conform to the United Nations Convention on the Rights of Persons with Disabilities and includes policy guidance, strategic blueprints, and budgeting and funding advice.

Policy Considerations

Governments and education policymakers can help advance the use of accessible technologies in schools and promote innovation in inclusive education by focusing on these priorities:

- **UPDATE GOVERNMENT POLICIES** National education authorities and ministries should work to update national and regional policies to promote the use of accessible technology in education.
- **INCORPORATE ACCESSIBLE TECHNOLOGIES IN CLASSROOMS** This includes adopting school technology procurement policies that reference international technical accessibility standards, ensure technology neutrality, allow for flexibility in design, permit both built-in and third-party solutions, and consider the total cost of ownership.
- **ENSURE FULL USE OF EXISTING ACCESSIBILITY FEATURES** Most mainstream technology tools that are used in schools—such as computers, tablets, and PCs—have a wealth of features and allow for personalized settings that can help students access curricula and collaborate with peers. Making full use of these features can vastly improve accessibility in education.
- **IMPROVE TEACHER TRAINING AND SUPPORT** Teachers need additional skills and knowledge to understand the value of accessible technology in the classroom. Educational authorities and ministries should provide awareness and skills training for all teachers.
- **STAY CURRENT WITH NEW TECHNOLOGIES** To help make education more engaging and inclusive, governments and educators should stay current with technology trends such as mobile learning, cloud-based solutions, touch screens, interactive user interfaces, and the use of game consoles for learning.

An Association of Accessibility Professionals

Key Points

- The technology industry is working to address the needs of people with disabilities and temporary impairments, but many organizations are either unaware of the available accessibility tools or they lack the expertise to use those tools.
- Accessibility has been advanced primarily by self-taught practitioners without the benefit of internationally recognized standards, professional certifications, or a pipeline of university-trained developers and engineers with expertise in accessibility.
- Without an international community of trained accessibility experts who share a body of knowledge and can help educate businesses, it will be difficult to further advance the cause within the technology industry.
- Microsoft is taking a leadership role in the formation of the International Association of Accessibility Professionals (IAAP), which aims to transform accessibility from a grassroots effort into an internationally recognized profession.

As technology becomes an increasingly vital part of everyday life, more devices, services, and software now incorporate accessibility features. But innovation in this area has been piecemeal, and accessibility remains an afterthought for many organizations that rely on or produce technology, for a number of reasons:

Many organizations do not fully understand the mainstream value generated by investments in accessibility features and technologies.

The adoption of accessible technologies has been hindered by the cost and complexity of integrating them into existing devices and software, and there are limited venues for professionals to share information or offer peer support.

Corporations, governments, and educational institutions that want to make their devices, services, and software accessible have difficulty finding designers and developers with sufficient expertise in this area.

There are no internationally accepted professional standards or curricula related to accessibility with which to guide and train developers and engineers.

Microsoft Approach

The technology industry, accessibility advocates, and government leaders have been struggling for years to find more effective ways to encourage the development of innovative accessibility solutions in devices, services, and software. In 2011, Microsoft participated in a year-long study (with support from the U.S. Department of Labor's Office of Disability Employment Policy), whose findings support the conclusion that an international association of accessibility professionals would be a step in the right direction. Microsoft is taking a leadership role in the formation of the International Association of Accessibility

Professionals (IAAP), which will provide the strategic leadership, global perspective, and sustained investment needed to transform accessibility into an internationally respected and recognized profession. The diverse array of founding members includes companies and organizations such as AT&T, Barclays, Scotiabank, Adobe, Hewlett-Packard, AbilityNet, and Ai Squared.

The major goals of the organization are:

- To create a globally recognized set of training materials related to accessibility. These could be organized as separate courses for business leaders, designers, developers, and other professions.
- To create a global community of individuals and organizations that spreads awareness of the need for accessible technology and offers resources to support the accessibility profession.
- To provide a global forum for accessibility professionals to share information, offer peer support, and track accessibility-related developments in technology and public policy.
- To develop and administer one or more professional accessibility certifications and offer continuing education to help practitioners augment their expertise as the field evolves.

The IAAP's mission, strategic objectives, governance structure, and other details have been finalized, and the association plans to launch and begin accepting members in the spring of 2014.

Policy Considerations

Policymakers can raise awareness of the need for accessible technology and encourage the development of resources for developers and engineers by focusing on the following priorities:

- **SUPPORT IAAP MEMBERSHIP AND EFFORTS** Policymakers should encourage organizations and businesses to join the IAAP and support the effort to build a globally recognized accessibility profession.
- **MAKE THE CASE FOR ACCESSIBILITY** Policymakers are in a unique position to promote digital inclusion and can help corporations, government entities, and educational institutions understand the broader societal value and economic benefits of investing in accessible technology and accessibility professionals.
- **PROMOTE THE NEED FOR TRAINED PROFESSIONALS** Recognizing the shortage of accessibility experts is the first step toward promoting investment in training and resources for developers and engineers. Policymakers can promote dialogue about this shortage and the need for a supported profession.
- **ENCOURAGE PUBLIC-PRIVATE PARTNERSHIPS** Governments, industry, and consumer advocacy organizations can deliver the greatest benefits in the area of accessibility through collaboration to establish appropriate principles and professional standards.

Implementing the U.N. Convention on the Rights of Persons with Disabilities

Key Points

- About 15 percent of the global population lives with some form of disability, according to the World Health Organization.
- The United Nations Convention on the Rights of Persons with Disabilities (CRPD) advances the rights of people with disabilities and includes digital accessibility as a prerequisite to enjoying all human rights and fundamental freedoms.
- Microsoft supports the effective implementation of the CRPD, and it works with industry trade groups and nongovernmental organizations to advance the goals of the treaty.
- Governments should look to global best practices and globally harmonized standards in creating accessibility policies and programs that broaden digital inclusion.

The United Nations Convention on the Rights of Persons with Disabilities (CRPD) is an international human rights instrument whose purpose is "to promote, protect and ensure the full and equal enjoyment of all human rights and fundamental freedoms by all persons with disabilities, and to promote respect for their inherent dignity." As of late 2013, 158 countries had signed the treaty and 138 had ratified it. Parties are required to "adopt all appropriate legislative, administrative and other measures for the implementation of the rights recognized" in the treaty as well as to "take into account the protection and promotion of the human rights of persons with disabilities in all policies and programmes."

The CRPD includes accessibility of information and communications technology (ICT) as a prerequisite for people with disabilities to fully enjoy all human rights and fundamental freedoms. This is the first time that digital accessibility has been elevated as a requirement comparable to accessibility of other forms of information and communication, as well as accessibility of transportation and the physical environment.

The CRPD specifically addresses equal access to ICT in Article 9, which states, in part:

> *To enable persons with disabilities to live independently and participate fully in all aspects of life, States Parties shall take appropriate measures to ensure to persons with disabilities access, on an equal basis with others, to the physical environment, to transportation, to information and communications,* ***including information and communications technologies and systems,*** *and to other facilities and services open or provided to the public, both in urban and in rural areas. [emphasis added]*

Article 9 further states that parties "shall also take appropriate measures to…[p]romote access for persons with disabilities to new information and communications technologies and systems, including the Internet."

In defining "discrimination on the basis of disability" and "reasonable accommodation," Article 2 of the treaty states:

> *"Discrimination on the basis of disability" means any distinction, exclusion or restriction on the basis of disability which has the purpose or effect of impairing or nullifying the recognition, enjoyment or exercise, on an equal basis with others, of all human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field. It includes all forms of discrimination, including denial of reasonable accommodation;*
>
> *"Reasonable accommodation" means necessary and appropriate modification and adjustments not imposing a disproportionate or undue burden, where needed in a particular case, to ensure to persons with disabilities the enjoyment or exercise on an equal basis with others of all human rights and fundamental freedoms.*

Although ICT is not specifically mentioned in these definitions, it is integral to political, economic, social, cultural, and civil engagement, including participation in education and the workplace.

Microsoft Approach

Microsoft strongly supports effective implementation of the CRPD by governments that have signed and ratified it. Microsoft also collaborates with industry trade groups and other nongovernmental organizations to advance the broad deployment of accessible technologies and products.

One example of such collaboration is the Microsoft partnership with six leading international organizations to encourage the UN to consider disability and accessible technology explicitly in its future development plans. The partnership produced a report, "The ICT Opportunity for a Disability-Inclusive Development Framework," which serves as a roadmap for broad digital inclusion that includes persons with disabilities around the world. In addition to Microsoft, the partners were the Broadband Commission for Digital Development, the Global Initiative for Inclusive ICTs (G3ict), International Disability Alliance, International Telecommunications Union (ITU), Telecentre.org Foundation, and UNESCO.

Microsoft also promotes accessibility and personalization in its products and services. For example, Windows 8 can be used on touch-only devices. And, like Office 2013, it includes touch-friendly accessibility features such as Narrator and Magnifier. Office 2013 also includes the Accessibility Checker, which helps users create an Office document that someone with a disability can easily read and access.

Policy Considerations

Governments and policymakers can advance effective implementation of the CRPD by focusing on these priorities:

- **CREATE PROGRAMS BASED ON INTERNATIONAL BEST PRACTICES** Countries that have signed or ratified the CRPD should look to global best practices, such as those created by G3ict and other international organizations, when they create accessibility policies and programs.
- **BROADEN DIGITAL INCLUSION THROUGH FOCUSED POLICIES AND PROGRAMS** Governments should work to make their own websites accessible and ensure that their education systems address the needs of students with disabilities.
- **CREATE POLICIES THAT COMPLEMENT GLOBAL STANDARDS** Accessibility policies and programs should reference globally harmonized accessibility standards to ensure a robust ecosystem of interoperable technologies and promote innovation.

Technology and Older Adults

Key Points

- As people age, vision, hearing, and dexterity impairments can affect their computer use. Tools and features that address these issues and allow personalization can make it easier and more comfortable for older adults to see, hear, and use their computers and other devices.
- Microsoft helps address the computing needs of older adults by building accessibility features into its products, offering training resources, and collaborating with organizations that help older adults use technology to maintain independence, productivity, connectivity, and enjoyment.
- Microsoft offers educational resources about safety and security to help older adults learn how to use computers more proficiently, avoid online scams, and make their computers more secure.
- Microsoft supports the work of governments to help promote digital inclusion, ensure technology neutrality, and promote interoperability among accessible technology products.

Older adults are increasingly embracing the digital world. According to a Pew Research Center study, as of February 2012, one-third (34 percent) of Internet users age 65 and older use social networking sites such as Facebook, and 18 percent do so on a typical day. As more people use computers and interact online, it is increasingly important that technology be accessible to everyone, regardless of age or ability level.

34% of Internet users age 65 and older use social networking sites such as Facebook

AND

18% do so on a typical day

By age 50, many people have vision, hearing, or dexterity impairments that can affect their use of technology. For example, persons with low vision may have difficulty seeing default screen fonts or may experience increased visual fatigue. Those with discomfort in their hands and arms may have difficulty typing or using a mouse for long periods.

Accessibility options and assistive technologies can help these users improve their computer experience by enabling them to adjust display, mouse, keyboard, sound, and speech options. Education and training can help older adults learn how to use computers more proficiently, avoid online scams, and make their computers more secure by installing antivirus software and setting up automatic updates.

Microsoft Approach

Microsoft is committed to making the benefits of technology and the digital world available and accessible to people of all ages through products, training, and collaboration.

Many Microsoft products include options that promote accessibility and personalization. For example, older people with vision impairments can benefit from the Narrator and Magnifier tools in Windows 8 and the various display features in Office 2013.

Microsoft provides training through tutorial materials and participation in events and conferences:

THE MICROSOFT ACCESSIBILITY WEBSITE provides demos, tutorials, and guidance on how to make computers easier to see, hear, and use.

THE MICROSOFT DIGITAL LITERACY PROGRAM helps novice computer users become proficient in basic computing skills.

THE MICROSOFT SAFETY & SECURITY CENTER provides guidance for safer Internet use. Brochures such as "Stay Safer on the Internet" include advice specifically for older computer users.

Microsoft collaborates with organizations such as AARP and SeniorNet to better understand and meet the needs of older adults. Microsoft also partners with governments, standards organizations, and the technology industry to help shape policy and solve shared challenges in making technology easier to use.

Policy Considerations

Governments can help advance digital inclusion for older adults by promoting the following policies:

- **ENSURE TECHNOLOGY NEUTRALITY** Establish technology-neutral policies that do not favor one technology over another and that help lead to greater innovation, eliminate barriers to trade and market access, encourage enhanced competition, and prevent bias in government procurement.

- **SUPPORT INTEROPERABILITY** Interoperability among systems is a key contributor to accessibility. Public policies should promote interoperability and allow technology vendors and purchasers to choose the solutions that best meet their needs.

Resources

GENERAL

Microsoft Accessibility: **www.microsoft.com/enable**

Microsoft Accessibility Update newsletter:

www.microsoft.com/enable/news/subscribe/default.aspx

Microsoft Safety & Security Center: **www.microsoft.com/security**

Microsoft Digital Literacy program: **www.microsoft.com/digitalliteracy**

Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations:

www.issuu.com/ewipublications/docs/russia-us-terminology/1?e=9392629/5358103

ACCESSIBILITY IN EDUCATION

Microsoft Accessibility in Education: **www.microsoft.com/enable/education**

ACCESSIBILITY PROFESSIONALS

International Association of Accessibility Professionals: **www.accessibilityassociation.org**

Assistive Technology Industry Association: **www.atia.org**

ACCESSIBILITY AND OLDER ADULTS

Microsoft Accessibility Guide for Individuals with Age-Related Impairments:

www.microsoft.com/enable/aging

SeniorNet: **www.seniornet.org**

GLOBAL INITIATIVES AND PARTNERSHIPS

UN Convention on the Rights of Persons with Disabilities:

www.un.org/disabilities/default.asp?id=259

e-Accessibility Policy Toolkit for Persons with Disabilities: **www.e-accessibilitytoolkit.org**

Global Initiative for Inclusive ICTs (G3ict): **www.g3ict.org**

Trust for the Americas: **www.poeta-accesible.org**

This material is provided for informational purposes only. Microsoft makes no warranties, express or implied. June 2014.